HP StorageWorks

Enterprise File Services WAN Accelerator Management Console 1.2

user's guide

392359–001

Part number: 392359-001
First edition: May 2005

Enterprise File Services WAN Accelerator Management Console User's Guide

Contents

Introduction

In This Introduction

Welcome to the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*. Read this introduction for an overview of the information provided in this guide and for an understanding of the documentation conventions used throughout. This introduction contains the following sections:

About This Guide

The *HP StorageWorks Enterprise File Services WAN Accelerator Management Console User's Guide* describes how to manage and monitor the HP StorageWorks Enterprise File Services WAN Accelerator using the HP EFS WAN Accelerator Management Console (Management Console).

Types of Users

This guide is written for storage and network administrators with familiarity administering and managing networks using Common Internet File System (CIFS), HyperText Transport Protocol (HTTP), File Transfer Protocol (FTP), and Microsoft Exchange.

Organization of This Guide

The *HP StorageWorks Enterprise File Services WAN Accelerator Management Console User's Guide* includes the following chapters:

- Chapter 1, "Overview of the HP EFS WAN Accelerator Management Console," describes how to connect to and navigate in the Management Console.

- Chapter 2, "Using the HP EFS WAN Accelerator Management Console," describes how to administer and manage the HP EFS WAN Accelerator using the Management Console.
- Appendix A, "HP EFS WAN Accelerator Ports," provides a list of the default ports, and interactive, and secure ports that are automatically forwarded by the HP EFS WAN Accelerator.

A glossary of terms follows the chapters, and a comprehensive index directs you to areas of particular interest.

Document Conventions

This manual uses the following standard set of typographical conventions to introduce new terms, illustrate screen displays, describe command syntax, and so forth.

Convention	Meaning
italics	Within text, new terms and emphasized words appear in italics.
boldface	Within text, commands, keywords, identifiers (names of classes, objects, constants, events, functions, program variables), environment variables, filenames, Graphical User Interface (GUI) controls, and other similar terms appear in boldface.
`Courier`	Information displayed on your terminal screen and information that you are instructed to enter appear in a Courier font.
KEYSTROKE	Keys that you are to press appear in uppercase letters in Helvetica font.

Hardware and Software Dependencies

The following table summarizes the hardware, software, and operating system requirements for the Management Console.

HP EFS WAN Accelerator Component	Hardware Requirements	Software Requirements Operating System Requirements
HP EFS WAN Accelerator Management Console	• Any computer that supports a Web browser with color image display.	• The Management Console has been tested with Mozilla, version, 1.2.1 and Microsoft Internet Explorer version 6.0x. NOTE: Javascript and cookies must be enabled in your browser. NOTE: If you want to encrypt your communication, you must have a Secure Sockets Layer (SSL) capable browser.

Ethernet Network Compatibility

The HP EFS WAN Accelerator supports the following types of Ethernet networks:

- Fast Ethernet (IEEE 802.3u 100 BaseTX)
- Gigabit Ethernet over Copper (IEEE 802.3ab 1000 Base-T)

In-path, HP EFS WAN Accelerator ports are Fast Ethernet, Ethernet auto-sensing.

The primary port in the HP EFS WAN Accelerator is 10/100/1000 Mbps auto-sensing. The HP EFS WAN Accelerator supports Jumbo Frames.

The HP EFS WAN Accelerator supports VLAN 802.1q. It does not support the Cisco InterSwitch Link (ISL) protocol.

Antivirus Compatibility

The HP EFS WAN Accelerator has been tested with the following antivirus software with no impact on performance:

- Network Associates (McAfee) VirusScan 7.0.0 Enterprise on the server
- Network Associates (McAfee) VirusScan 7.1.0 Enterprise on the server
- Network Associates (McAfee) VirusScan 7.1.0 Enterprise on the client
- Symantec (Norton) AntiVirus Corporate Edition 8.1 on the server

The HP EFS WAN Accelerator has been tested with the following antivirus software with a noticeable to moderate impact on performance:

- F-Secure Anti-Virus 5.43 on the client
- F-Secure Anti-Virus 5.5 on the server
- Network Associates (McAfee) NetShield 4.5 on the server
- Network Associates VirusScan 4.5 for multiplatforms on the client
- Symantec (Norton) AntiVirus Corporate Edition 8.1 on the client

Additional Resources

This section describes the following resources that supplement the information in this guide:

- Release notes
- Related HP documentation
- Related technical reference books

Related HP Documentation

You can access the complete document set for the HP EFS WAN Accelerator from the *HP EFS WAN Accelerator Documentation Set CD-ROM*:

- *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide* describes how to install and configure the HP EFS WAN Accelerator.
- *HP EFS WAN Accelerator Command Line Interface Reference Manual* is a reference manual for the HP EFS WAN Accelerator command-line interface for the HP EFS WAN Accelerator. It lists commands, syntax, parameters, and example usage.
- *HP StorageWorks Enterprise File Services WAN Accelerator Manager User's Guide* describes how to install, configure, and administer a network made up of multiple HP EFS WAN Accelerators using the HP StorageWorks Enterprise File Services WAN Accelerator Manager.

Online Documentation

The HP EFS WAN Accelerator documentation set is periodically updated with new information. To access the most current version of the HP EFS WAN Accelerator documentation and other technical information, consult the HP support site located at **http://www.hp.com**.

Related Reading

To learn more about network storage systems and network administration, consult the following books:

- *Microsoft Windows 2000 Server Administrator's Companion* by Charlie Russell and Sharon Crawford (Microsoft Press, January 2000)
- *Common Internet File System (CIFS) Technical Reference* by the Storage Networking Industry Association (Storage Networking Industry Association, 2002)
- *TCP/IP Illustrated, Volume I, The Protocols* by W. R. Stevens (Addison-Wesley, 1994)
- *Internet Routing Architectures* (2nd Edition) by Bassam Halabi (Cisco Press, 2000)

Contacting HP

This section describes how to contact departments within HP.

NOTE: Do not load any other software on your HP StorageWorks EFS WAN Accelerator, as doing so will void your support agreement and you will not be able to receive HP technical support.

Internet

You can find out about HP products through our web site at **http://www.hp.com**.

Technical Support

Telephone numbers for worldwide technical support are listed on the following HP web site: http://www.hp.com/support. From this web site, select the country of origin. For example, the North American technical support number is 800-633-3600.

NOTE: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Web Site

The HP web site has the latest information on this product, as well as the latest drivers. Access the storage site at: http://www.hp.com/country/us/eng/prodserv/storage.html. From this web site, select the appropriate product or solution.

HP NAS Services Web Site

The HP NAS Services site allows you to choose from convenient HP Care Pack Services packages or implement a custom support solution delivered by HP ProLiant Storage Server specialists and/or our certified service partners. For more information see us at http://www.hp.com/hps/storage/ns_nas.html.

CHAPTER 1

Overview of the HP EFS WAN Accelerator Management Console

In This Chapter

This chapter introduces the HP EFS WAN Accelerator Management Console (Management Console). This chapter includes the following sections:

NOTE: If you prefer, you can use the HP EFS WAN Accelerator command-line interface (CLI) to perform configuring and monitoring tasks. For detailed information, see the *HP EFS WAN Accelerator Command Line Interface Reference Manual*.

This chapter assumes you have installed and configured the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

Connecting to the Management Console

You can connect to the Management Console through any supported Web browser.

Connecting to the Management Console

To connect to the Management Console you must know the Uniform Resource Locator (URL) and administrator password that you assigned during the initial setup of the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

NOTE: Cookies and Javascript must be enabled in your Web browser.

To connect to the Management Console

1. Enter the URL for the Management Console in the location box of your Web browser:

protocol://*host.domain*

protocol is **http** or **https**. HyperText Transport Protocol Secure (HTTPS) uses the Secure Sockets Layer (SSL) protocol to ensure a secure environment. If you use HTTPS to connect, you are prompted to inspect and verify the SSL key.

host is the host name you assigned the HP EFS WAN Accelerator during initial configuration. If your DNS server maps that IP address to a name, you can specify the DNS name.

domain is the full domain name for the appliance.

TIP: Alternatively, you can specify the IP address instead of the host and domain name.

The Management Console appears, displaying the Welcome page.

Figure 1-1. Welcome Page

2. In the **Account** text box, type the user login: **admin**, **monitor**, or a login from a Remote Authentication Dial-In User Service (RADIUS), or a Terminal Access Controller Access Control System (TACACS+) database. The default login is **admin**.

   Users with administrator **(admin**) privileges can configure and administer the HP EFS WAN Accelerator. Users with monitor (**monitor**) privileges can view connected HP EFS WAN Accelerators and performance reports.

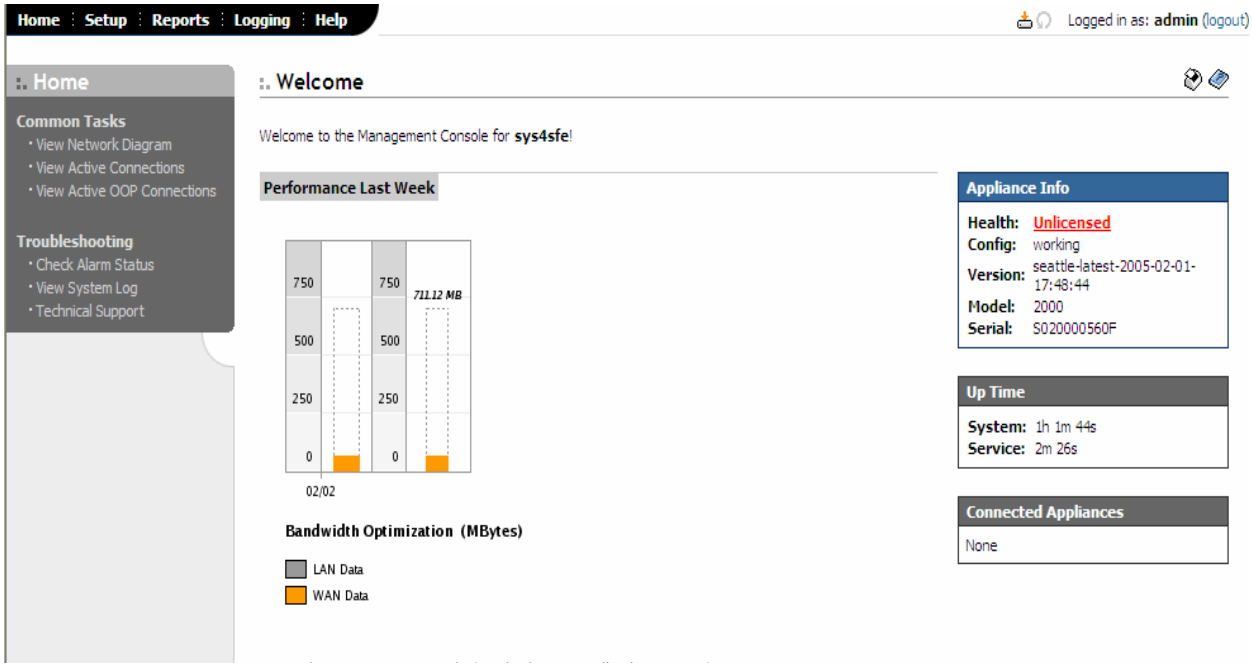
3. In the **Password** text box, type the password you assigned when you performed the initial set up the HP EFS WAN Accelerator. (The HP EFS WAN Accelerator is shipped with the default password: **password**.)

4. Click **Login** to display the Home: Welcome page. The Home: Welcome page summarizes the current status of your system and provides links to a network diagram, active connections, out-of-path connections, alarm status, system logs, and technical support.

The Home: Welcome Page

The Management Console Home: Welcome page includes the current status of the appliance and the Performance Last Week report.

Figure 1-2. Home: Welcome Page



The Performance Last Week report summarizes the bandwidth optimization for your Local Area Network (LAN) and Wide Area Network (WAN) traffic using the HP EFS WAN Accelerator.

The **Appliance Info**, **Up Time**, and **Connected Appliances** boxes display the following information for the HP EFS WAN Accelerator.

Field	Description
Health	The current status of the system. The HP EFS WAN Accelerator can be in one of the following states: • **Healthy**. All HP EFS WAN Accelerator systems are functioning properly. • **Degraded**. An HP EFS WAN Accelerator alarm has been triggered. Alarms are triggered for software version mismatches, abnormal memory page swapping activity, when the CPU utilization threshold has been reached, or on the Models 5000 and 3000, if there is a RAID (Redundant Array of Independent Disks) issue. • **Critical**. The HP EFS WAN Accelerator service is not functioning or the HP EFS WAN Accelerator is in bypass mode • **Unlicensed**. The HP EFS WAN Accelerator does not have a a base license key or the key has expired. • **Corrupted Store**. The HP EFS WAN Accelerator data store is corrupt. To clear the data store, see "Starting, Stopping, and Restarting the HP EFS WAN Accelerator Service" on page 94. • **Service Halted**. The HP EFS WAN Accelerator has detected a software error that prevents the HP EFS WAN Accelerator service from continuing. The HP EFS WAN Accelerator service shuts down and remains shutdown. You must contact technical support at **http://www.HP.com** if this alarm occurs. **Note**: For unhealthy states, click the link to go to the Reports: Alarms Status page.
Config	The name of the current running configuration. If you activate another configuration or save your new configuration settings, the new name is reflected here.
Version	The software version number that is currently installed on the HP EFS WAN Accelerator.
Model	The model number of the HP EFS WAN Accelerator.
Serial	The serial number for the HP EFS WAN Accelerator.
System	Total time the system has been active.
Service	The state of the HP EFS WAN Accelerator service. The total time the HP EFS WAN Accelerator has been running or **Not Running** is displayed. To restart the HP EFS WAN Accelerator service, see "Starting, Stopping, and Restarting the HP EFS WAN Accelerator Service" on page 94.
Connected Appliances	The host names of connected HP EFS WAN Accelerators.

Navigating in the Management Console

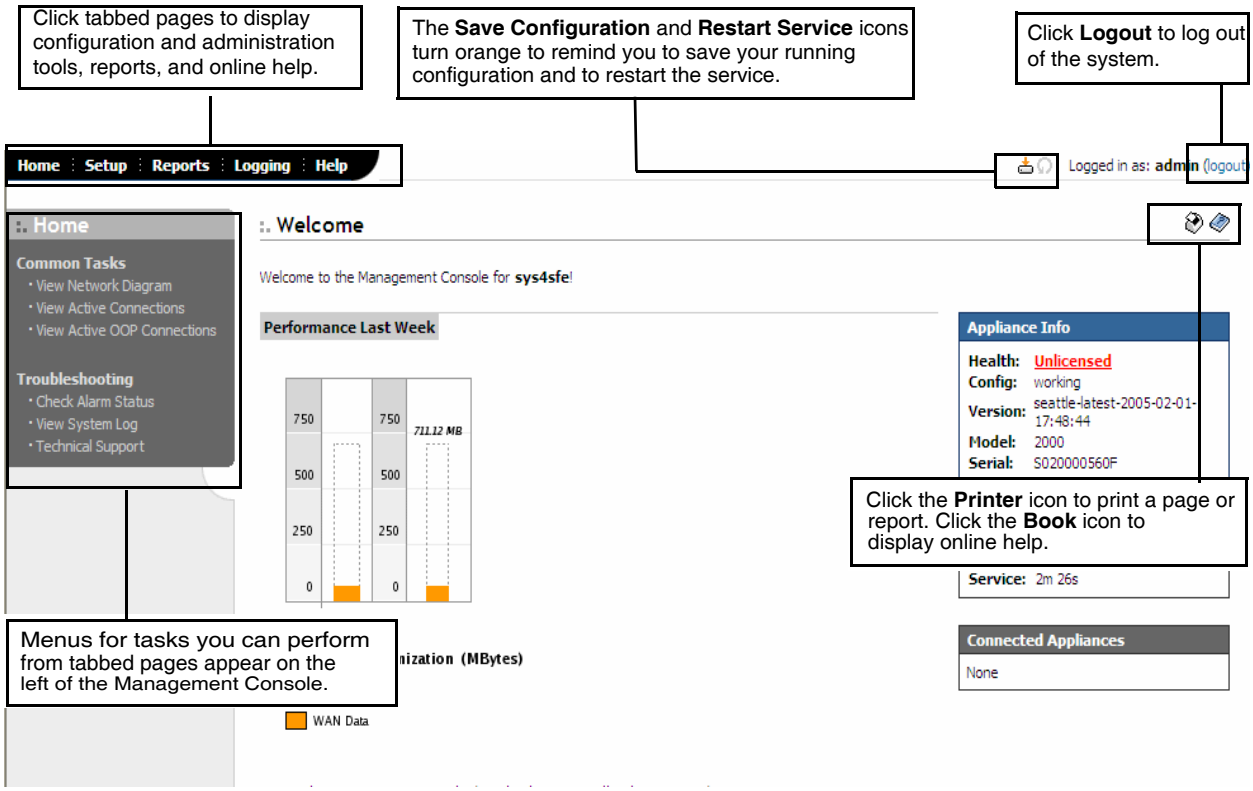
The following section describes how to navigate in the Management Console.

Navigating in the Management Console

You navigate to the tools and reports available to you in the Management Console using hyperlinked tabs and menus.

The following figure illustrates the tabs and menus that appear on each page of the Management Console.

Figure 1-3. Management Console, Home: Welcome Page



TIP: You can revisit the Home: Welcome page by clicking Home in the navigation bar.

Tabbed Pages and Menus

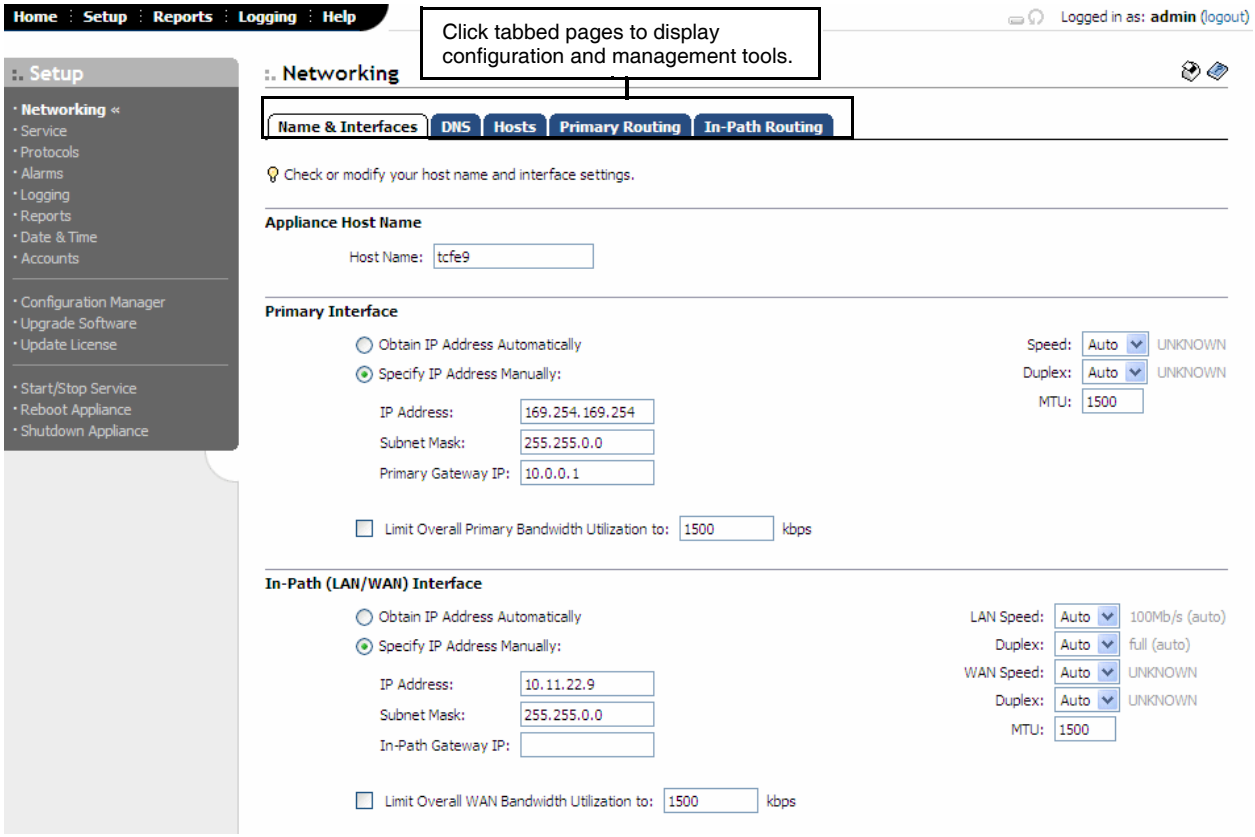
Figure 1-3 shows the tabbed pages that appear on each page of the Management Console. You click the hyperlinked tabs to display tools and reports to help you monitor and manage your HP EFS WAN Accelerator. The following table summarizes the purpose of each tabbed page.

Tab	Purpose
Home	Display performance and system status and provide links to a network diagram, active connections, out-of-path connections, alarm status, system logs, and technical support. For details about these reports, see "Creating HP EFS WAN Accelerator Reports" on page 96.
Setup	Configure and administer the appliance. For details about the tools provided in this menu, see Chapter 2, "Using the HP EFS WAN Accelerator Management Console."
Reports	Create and view performance, network, and appliance reports. For details about these reports, see "Creating HP EFS WAN Accelerator Reports" on page 96.
Logging	View system logs. For details, see "Viewing HP EFS WAN Accelerator Logs" on page 115.
Help	Display contact information for technical support, the HP EFS WAN Accelerator command-line interface (CLI) commands, and the online-help table of contents. For details, see "Getting Help" on page 116.

When you click a hyperlinked tab, a menu for the tasks you can perform appears on the left of the Management Console. For example, when you click the Setup tab, the Setup menu appears.

Some of the pages also contain tabbed pages. For example, if you select Setup: Networking, tabbed pages appear as shown in Figure 1-4.

Figure 1-4. Setup: Networking Page



Menu items are hyperlinks to pages that display tools and reports to help you manage and administer your HP system. When you click a menu item, you display the primary tool or report for the menu choice.

Saving Your Configuration

As you **Apply** page settings, the values are applied to the running configuration, the **Save Configuration** icon changes to orange, and a save button appears in the left menu to remind you to permanently save your configuration settings to memory.

For detailed information about saving your configuration to memory, see "Managing Configurations" on page 83.

Restarting the HP EFS WAN Accelerator Service

Some configuration settings apply to the HP EFS WAN Accelerator service. The HP EFS WAN Accelerator service is a daemon that executes in the background performing operations when required.

If the new settings apply to the HP EFS WAN Accelerator Service, the **Restart Service** icon turns orange to remind you to restart the service. For detailed information, see "Starting, Stopping, and Restarting the HP EFS WAN Accelerator Service" on page 94.

Printing Console Pages and Reports

You can print Management Console pages and reports.

To print pages and reports

- Click the **Printer** icon in the upper right-side of the page to display a printer-friendly version of the page.

Displaying Online Help

You can view online help that describes each page of the Management Console and the tasks that you can perform. For the online help table of contents, see "Viewing Online Help Contents" on page 117.

To display online help

- Click the **Book** icon in the upper right-side of the page. The help for the page appears in a new browser window.

The Help tab provides you with the following links to help you administer and manage the HP EFS WAN Accelerator:

- **Technical Support**. HP technical support.
- **CLI Commands**. The HP EFS WAN Accelerator Command Line Interface.
- **Online Help.** A table of contents of the help topics in the Management Console.

For detailed information, see "Getting Help" on page 116.

Logging Out

Click the **Logout** link to end your session and require subsequent users to authenticate their session. When you click the **Logout** link, the Management Console displays the Good-Bye page.

To log out of the Management Console

- Click **Logout** to display the Good-Bye page and log out of the Management Console.

CHAPTER 2

Using the HP EFS WAN Accelerator Management Console

In This Chapter

This chapter describes how to administer and manage the HP EFS WAN Accelerator using the HP EFS WAN Accelerator Management Console (Management Console). This chapter includes the following sections:

This chapter assumes that you have installed and configured the HP EFS WAN Accelerator.

If you prefer, you can use the HP EFS WAN Accelerator command-line interface (CLI) to configure your system. For detailed information, see the *HP EFS WAN Accelerator Command Line Interface Reference Manual*.

IMPORTANT: As you finish entering values for each configuration page, click **Apply** to test your settings. When you **Apply** page settings, the values are applied to the running configuration—they are not saved permanently until you write them to memory. The **Save Configuration** icon turns orange to remind you to save your configuration. To write your configuration settings to memory, see "Managing Configurations" on page 83.

IMPORTANT: Some configuration settings apply to the HP EFS WAN Accelerator service. To apply the new settings, you must restart the HP EFS WAN Accelerator service. The **Restart Service** icon turns orange to remind you to restart the service. For detailed information, see "Starting, Stopping, and Restarting the HP EFS WAN Accelerator Service" on page 94.

Setting Network Parameters

The following section describes how to set the host and interface settings (primary, in-path, and auxiliary interfaces), Domain Name Service (DNS), hosts (if you are not using DNS to find hosts), primary routes (if your network requires additional static routing rules), and in-path routing. It contains the following sections:

Setting the Host Name and Interfaces

You set the following network parameters in the Setup: Networking, Network & Interfaces page:

Setting the Host Name and Primary Interface

During the initial configuration of the HP EFS WAN Accelerator, you assigned a host name, primary interface, and in-path interface to the appliance. Check or modify your settings in the Setup: Networking, Network & Interfaces page.

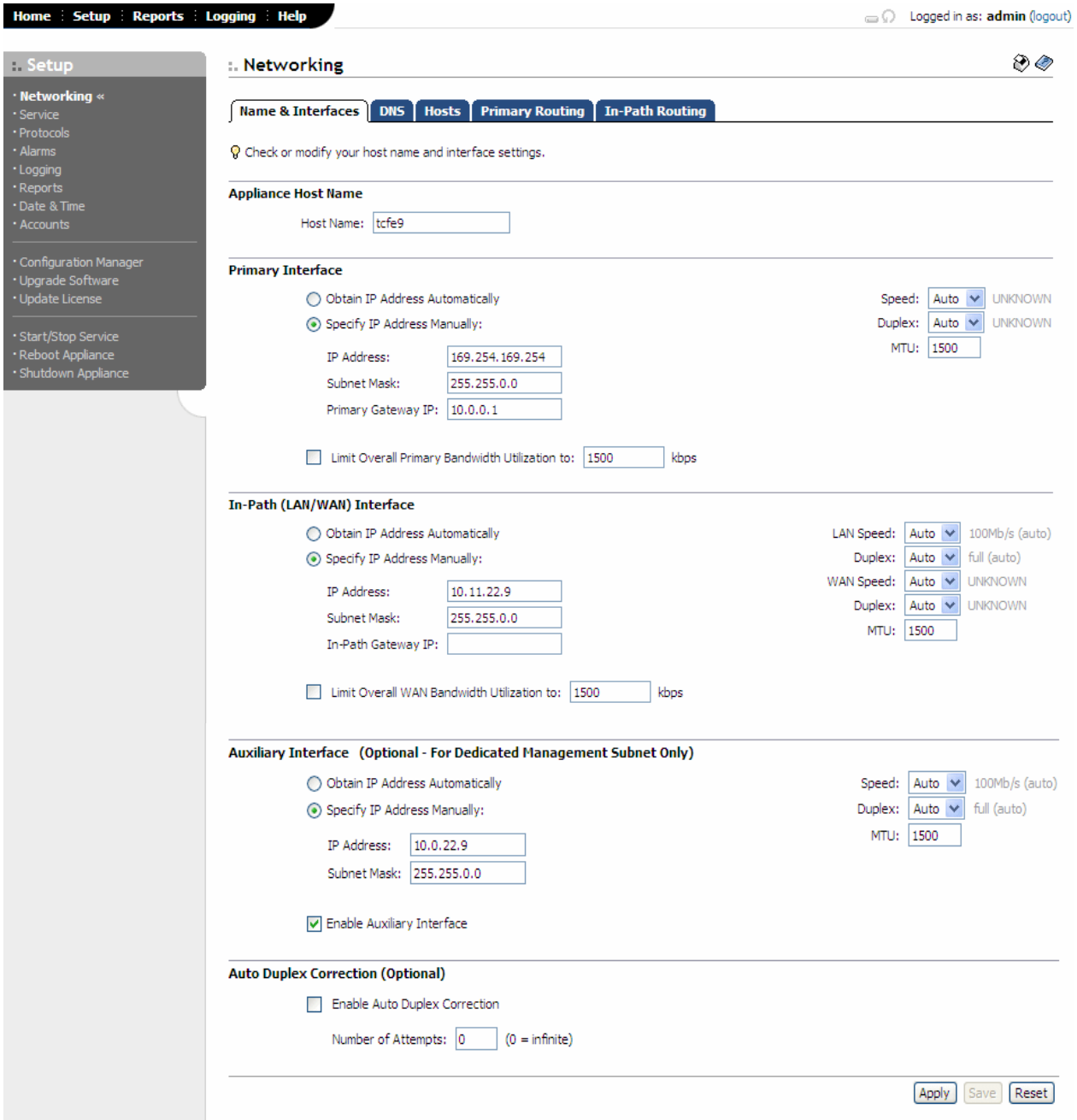
If your network routers or switches do not automatically negotiate the speed and duplex, you must manually set the speed and duplex for the primary interface.

IMPORTANT: The speed and duplex must match (LAN and WAN) in an in-path configuration. If they do not you are likely to have a large number of errors on the interface when it is in bypass mode, because the switch and router are not set with the same duplex settings.

To set the host name and primary interface

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

Figure 2-1. Setup: Networking, Name & Interfaces Page



2. Under Appliance Host Name, type a host name in the **Host Name** text box.

3. Under Primary Interface, choose the method for obtaining an IP address for the primary interface:

   - Click **Obtain an IP address Automatically** to have the HP EFS WAN Accelerator automatically find the IP address for the primary interface. (A Dynamic Host Configuration Protocol (DHCP) server must be available so that the HP EFS WAN Accelerator can request the IP address from it.)
   - Click **Specify IP Address Manually** to assign a specific appliance as the primary interface:
     - Type the IP address in the **IP Address** text box.
     - Type the subnet mask in the **Subnet Mask** text box.
     - Type the IP address for the primary gateway in the **Primary Gateway IP** text box. The primary gateway must be in the same network as the primary interface. You must set the primary gateway for in-path configurations.

4. Click **Limit Overall Primary Bandwidth Utilization to:** and type a value in the **kbps** text box to restrict the total optimized traffic to a specific bandwidth limit.

IMPORTANT: The bandwidth limit applies only to the outgoing WAN interface and outgoing packets, it does not apply to passed-through traffic. To limit a particular link to a certain bandwidth, you must set the limit on the client and the server HP EFS WAN Accelerator.

---

5. Click **1000**, **100**, or **10** in the **Speed** drop-down list to set the speed for the primary interface. The default value is **Auto**.

6. Click **Full** or **Half** in the **Duplex** drop-down list to set the duplex speed for the primary interface. The default value is **Auto**.

7. Type a Maximum Transmission Unit (MTU) value in the **MTU** text box. The MTU is the largest physical packet size, measured in bytes, that a network can transmit.

8. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)

9. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous value.

Setting In-Path Interfaces

During the initial configuration of the HP EFS WAN Accelerator, you assigned an in-path interface to the HP EFS WAN Accelerator. Check or modify your settings in the Setup: Networking, Network & Interfaces page.

You specify the in-path interface if you plan to have the HP EFS WAN Accelerator in the direct path (the same subnet) as the client and the server in your network. You also set the in-path gateway (WAN router).

IMPORTANT: If there is a routed network on the LAN-side of the in-path HP EFS WAN Accelerator, the router that is the default gateway for the HP EFS WAN Accelerator must not have the Access Control List (ACL) configured to drop packets from the remote hosts as its source. The in-path HP EFS WAN Accelerator uses IP masquerading to appear as the remote server.

Speed and Duplex Tips

If your network routers do not automatically negotiate the speed and duplex, you must manually set the speed and duplex for the in-path interface (that is, the HP EFS WAN Accelerator).

Speed and duplex mismatches can easily occur in your network. For example, if one end of the link is set at **half** or **full-duplex** and the other end of the link is configured to auto negotiate (**auto**), the link defaults to half-duplex, regardless of the duplex setting on the non-auto-negotiated end. This duplex mismatch passes traffic, but it causes interface errors and results in degraded optimization.

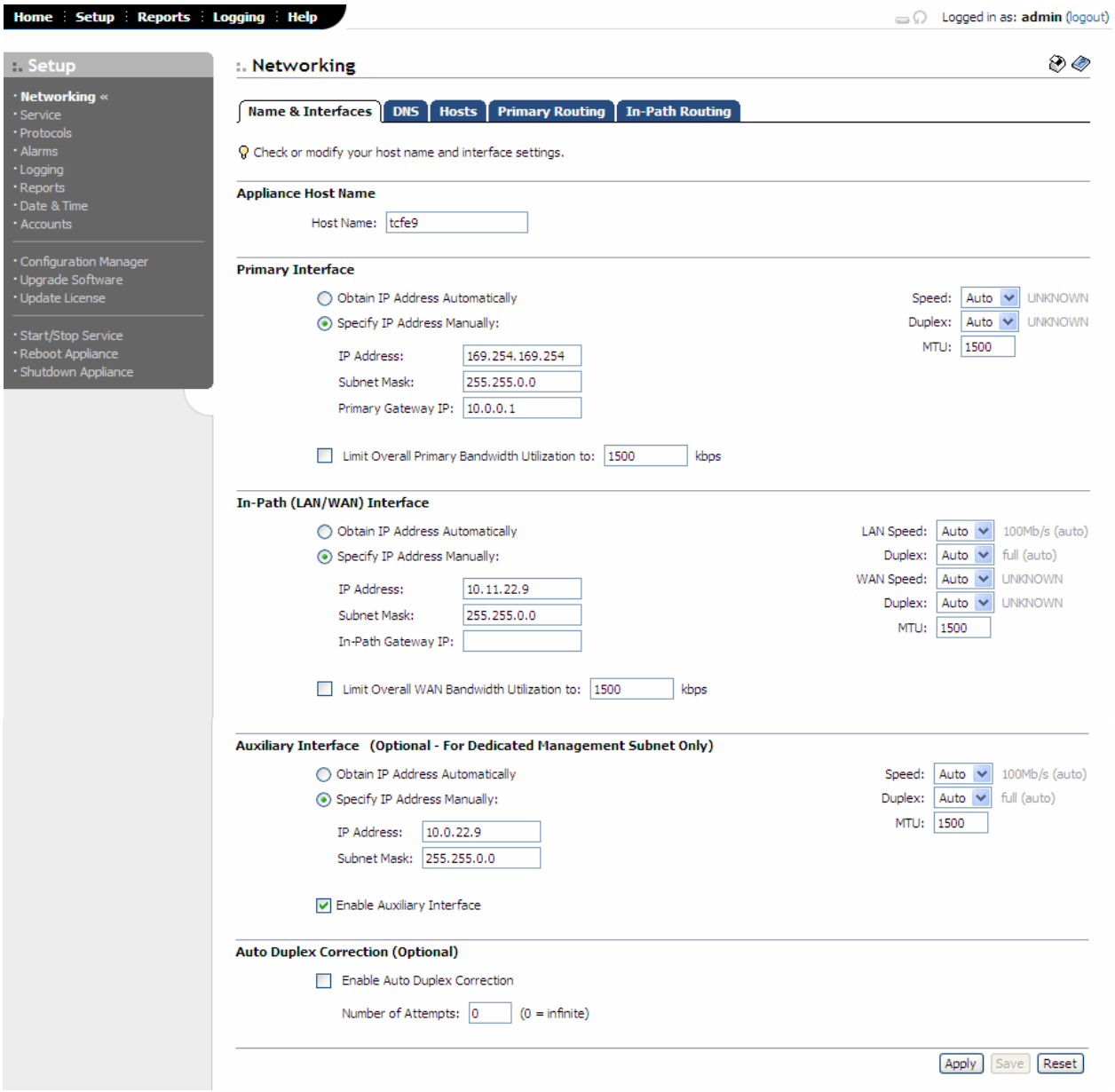
The following are general guidelines to avoid speed and duplex mismatches when configuring the HP EFS WAN Accelerator:

- If there is a serious problem with the HP EFS WAN Accelerator and it goes into bypass mode (that is, it automatically continues to pass traffic through your network), a speed and duplex mismatch might occur when you reboot the HP EFS WAN Accelerator. To avoid a speed and duplex mismatch, configure your LAN external pair to match the WAN external pair. For example, **auto=auto** or **100F=100F**. For detailed information about bypass mode, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
- Routers are often configured with fixed speed and duplex settings. Check your router configuration and set it to match the HP EFS WAN Accelerator WAN and LAN settings, then make sure your switch has the correct setting.
- After you finish configuring the HP EFS WAN Accelerator, check for speed and duplex error messages (**crc** or **frame** errors) in the Logging, View System Log page of the Management Console. For detailed information about displaying HP EFS WAN Accelerator logs, see "Viewing HP EFS WAN Accelerator Logs" on page 115.

To set the in-path interface

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

Figure 2-2. Setup: Networking, Name & Interfaces Page



2. Under In-Path Interface, choose the method for obtaining an IP address for the in-path interface:

   - Click **Obtain an IP address Automatically** to have the HP EFS WAN Accelerator automatically find the IP address for the in-path interface. (A DHCP server must be available so that the HP EFS WAN Accelerator can request the IP address from it.)
   - Click **Specify IP Address Manually** to assign a specific appliance as the in-path interface:
     - Type the IP address in the **IP Address** text box.

- Type the subnet mask in the **Subnet Mask** text box.
- Type the IP address for the in-path gateway in the **In-Path Gateway IP** text box. If you have a router (or a Layer-3 switch) on the LAN side of your network, you should specify this device as the in-path gateway.

3. Click **Limit Overall WAN Bandwidth Utilization to:** and type a value in the **kbps** text box to restrict the total optimized traffic to a specific bandwidth limit.

IMPORTANT: The bandwidth limit applies only to the outgoing WAN interface and outgoing packets, not to passed-through traffic. To limit a particular link to a certain bandwidth, you must to set the limit on the client and the server HP EFS WAN Accelerator.

---

4. Click **100**, or **10** in the **LAN Speed** drop-down list to set the speed for the in-path LAN port. The default value is **Auto**.
5. Click **Full**, or **Half** in the **Duplex** drop-down list to set the duplex speed for the in-path LAN port. The default value is **Auto**.
6. Click **100**, or **10** in the **WAN Speed** drop-down list to set the speed for the in-path WAN port. The default value is **Auto**.
7. Click **Full**, or **Half** in the **Duplex** drop-down list to set the duplex speed for the in-path WAN port. The default value is **Auto**.
8. Type an MTU value in the **MTU** text box. The MTU is the largest physical packet size, measured in bytes, that a network can transmit. The MTU is set once on the in-path interface, it propagates automatically to the LAN and the WAN.
9. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)
10. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Setting Auxiliary Interfaces

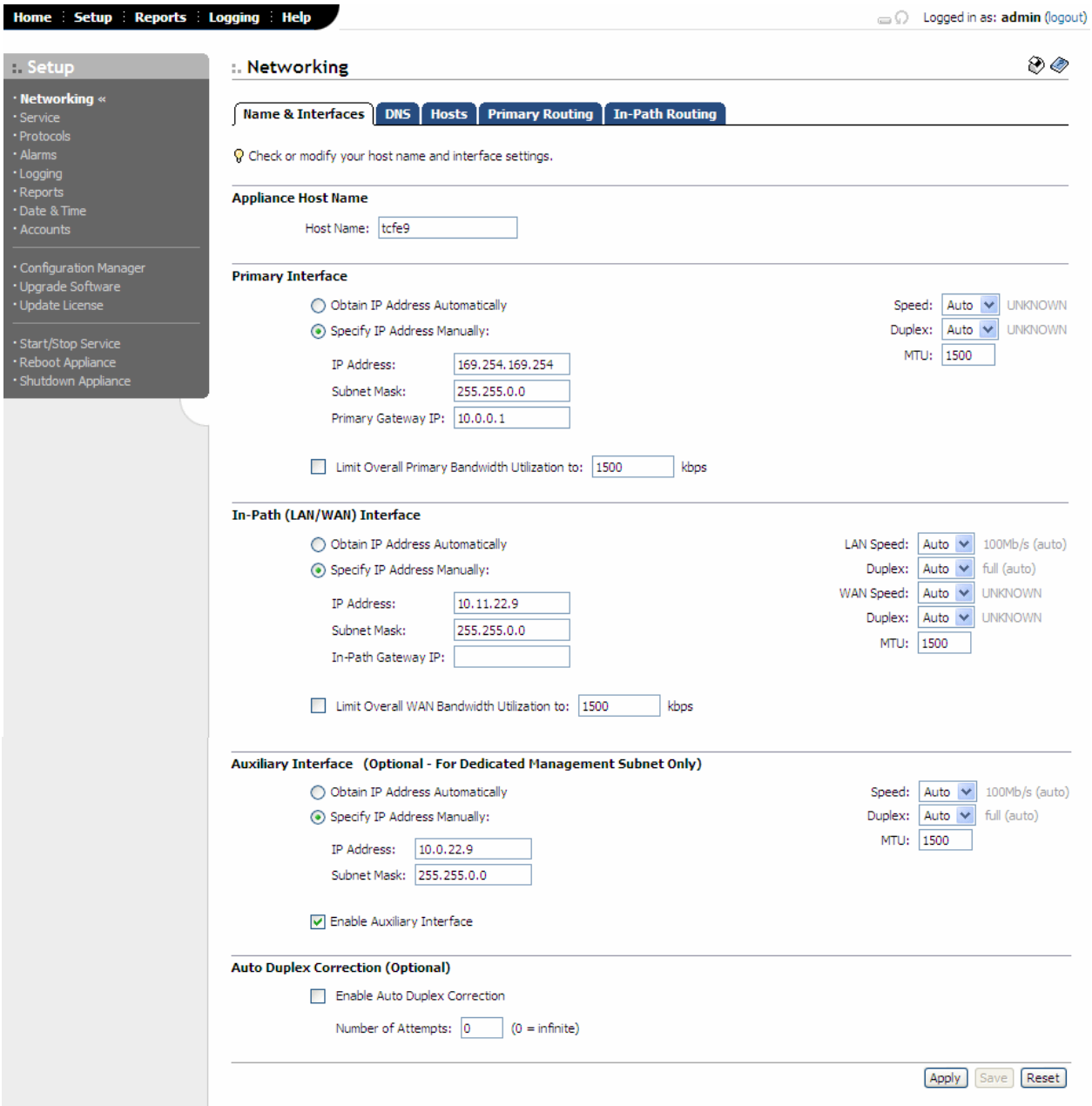
Optionally, you can set an auxiliary interface if your network configuration has a dedicated management subnet. For example, if your network has an auxiliary interface that connects and passes packets between the HP EFS WAN Accelerator and a different network such as one purely for device management.

If your network routers do not automatically negotiate the speed and duplex, you must manually set the speed and duplex for the auxiliary interface.

To set an auxiliary interface

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

Figure 2-3. Setup: Networking, Name & Interfaces Page



2. Optionally, under Auxiliary Interface, choose the method for obtaining the auxiliary interface IP address:

   - Click **Obtain an IP address Automatically** to have the HP EFS WAN Accelerator automatically find the IP address for the interface. (A DHCP server must be available so that the HP EFS WAN Accelerator can request the IP address from it.)
   - Click **Specify IP Address Manually** to assign a specific device as the interface:

- Type the IP address in the **IP Address** text box.
- Type the subnet mask in the **Subnet Mask** text box.

3. Click **1000**, **100**, or **10** in the **Speed** drop-down list to set the speed for the auxiliary interface. The default value is **Auto**.
4. Click **Full** or **Half** in the **Duplex** drop-down list to set the duplex speed for the auxiliary interface. The default value is **Auto**.
5. Type an MTU value in the **MTU** text box. The MTU is the largest physical packet size, measured in bytes, that a network can transmit.
6. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)
7. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Setting Automatic Duplex Correction

To automatically correct duplex mismatches, enable the automatic duplex correction feature in the Setup: Names & Interfaces page. The automatic correction feature functions only when the HP EFS WAN Accelerator is set at **auto** or **full-duplex**.

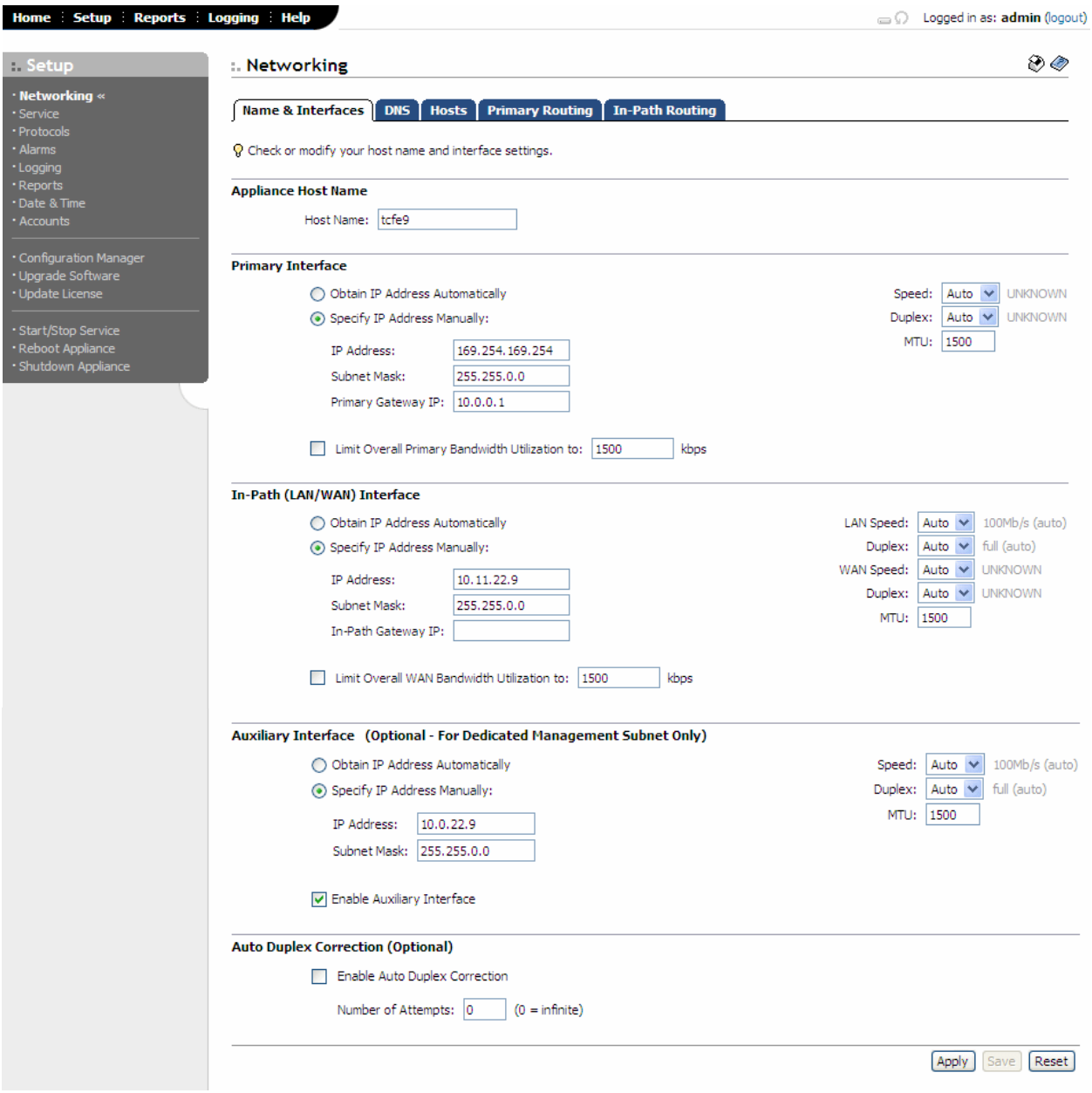
The HP EFS WAN Accelerator automatically detects and notifies you of duplex mismatches. A duplex mismatch passes traffic but optimization is degraded due to the high frequency of late packet collisions. If a duplex mismatch is detected, the HP EFS WAN Accelerator cycles through duplex settings for the interface, selecting the best configuration. After a duplex mismatch has been detected, a log message is recorded and email is sent.

For detailed information about configuring email notification, see "Setting Fault Notification" on page 65.

To set automatic duplex correction

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

Figure 2-4. Setup: Networking, Name & Interfaces Page



2. Click **Enable Auto Duplex Correction** and type a number in the **Number of Attempts** text box to set automatic duplex correction in the HP EFS WAN Accelerator. The **Number of Attempts** default value is **0**.

3. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)

4. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Setting the Domain Name Service

During the initial setup of the HP EFS WAN Accelerator you specified the primary Domain Name Service (DNS) server and domain for the appliance. Check or modify your settings in the Setup: Networking, DNS page.

NOTE: HP recommends you configure the Setup: Networking, DNS page.

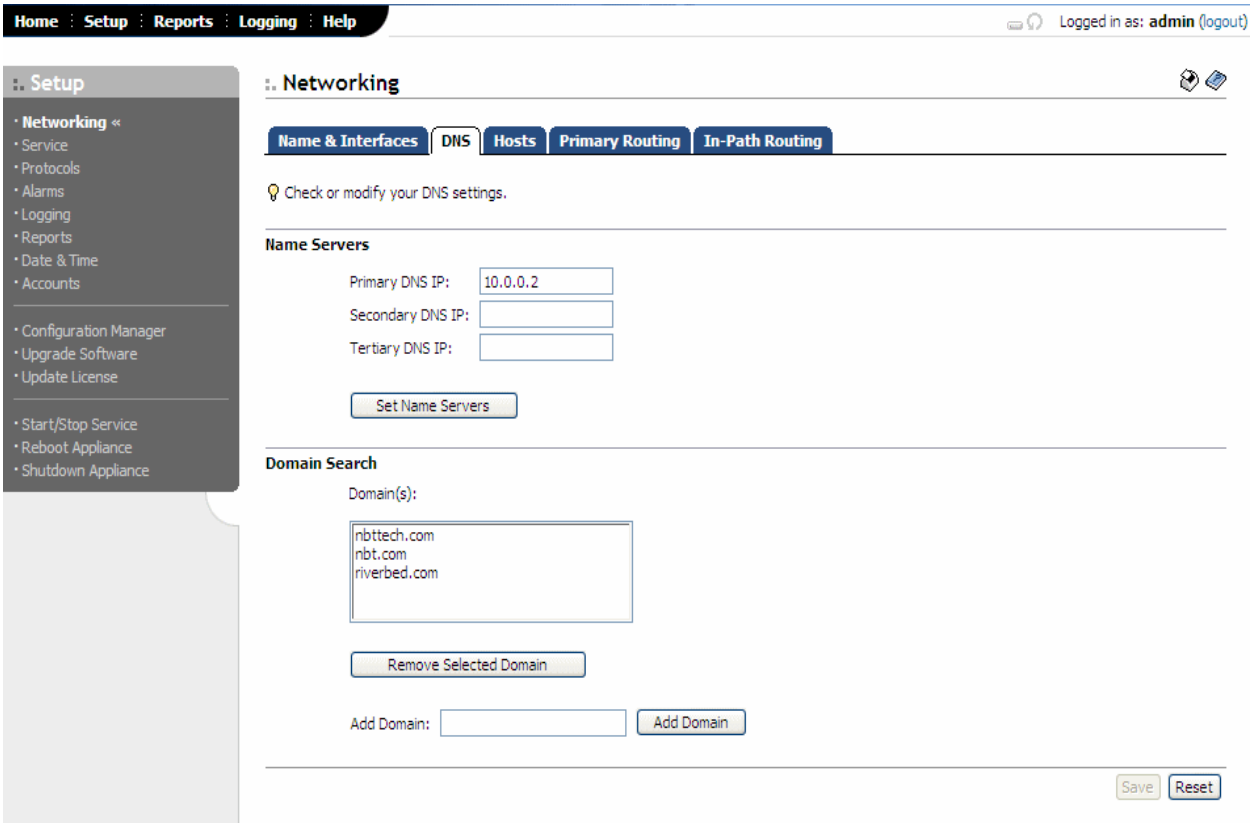
You can also set secondary and tertiary DNS name servers in the Setup: Networking, DNS page.

You can provide additional domains for which the HP EFS WAN Accelerator can search. If you specify domains in the **Domain Search** text box, the HP EFS WAN Accelerator automatically finds the appropriate domain for each of the hosts that you enter in the system.

To set the DNS server

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click the DNS tab to display the Setup: Networking, DNS page.

Figure 2-5. Setup: Networking, DNS Page



3. Under Name Servers, type the IP address for the primary name server in the **Primary DNS IP** text box.

4. Type the IP address for the secondary name server (if any) in the **Secondary DNS IP** text box.

5. Type the IP address for the tertiary name server (if any) in the **Tertiary DNS IP** text box.

6. Click **Set Name Servers** to apply your settings.

7. Under Domain Search, type a domain name in the **Add Domain** text box and click **Add Domain** to configure a domain for which the HP EFS WAN Accelerator will search. (To remove a domain name from the list, click **Remove Selected Domain**.)

8. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Specifying Hosts

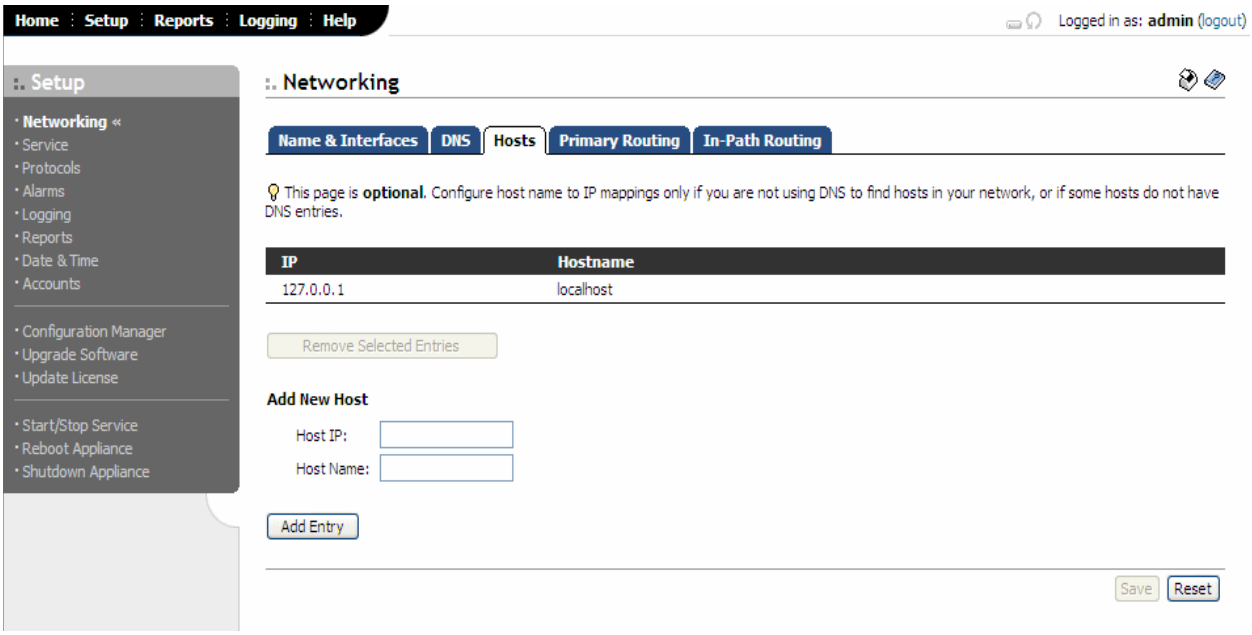
Optionally, specify hosts in the Setup: Networking, Hosts page if you are not using DNS to resolve host names and IP addresses in your system or if you want to override mapping for a host or IP address.

To specify a host

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

2. Click the Hosts tab to display the Setup: Networking, Hosts page.

Figure 2-6. Setup: Networking, Hosts Page



3. Under Add New Host, type the IP address for the new host in the **Host IP** text box.
4. Type the host name for the new host in the **Host Name** text box.
5. Click **Add Entry** to apply your settings to the running configuration.
6. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove a host, click the check box next to the name and click **Remove Selected Entries**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

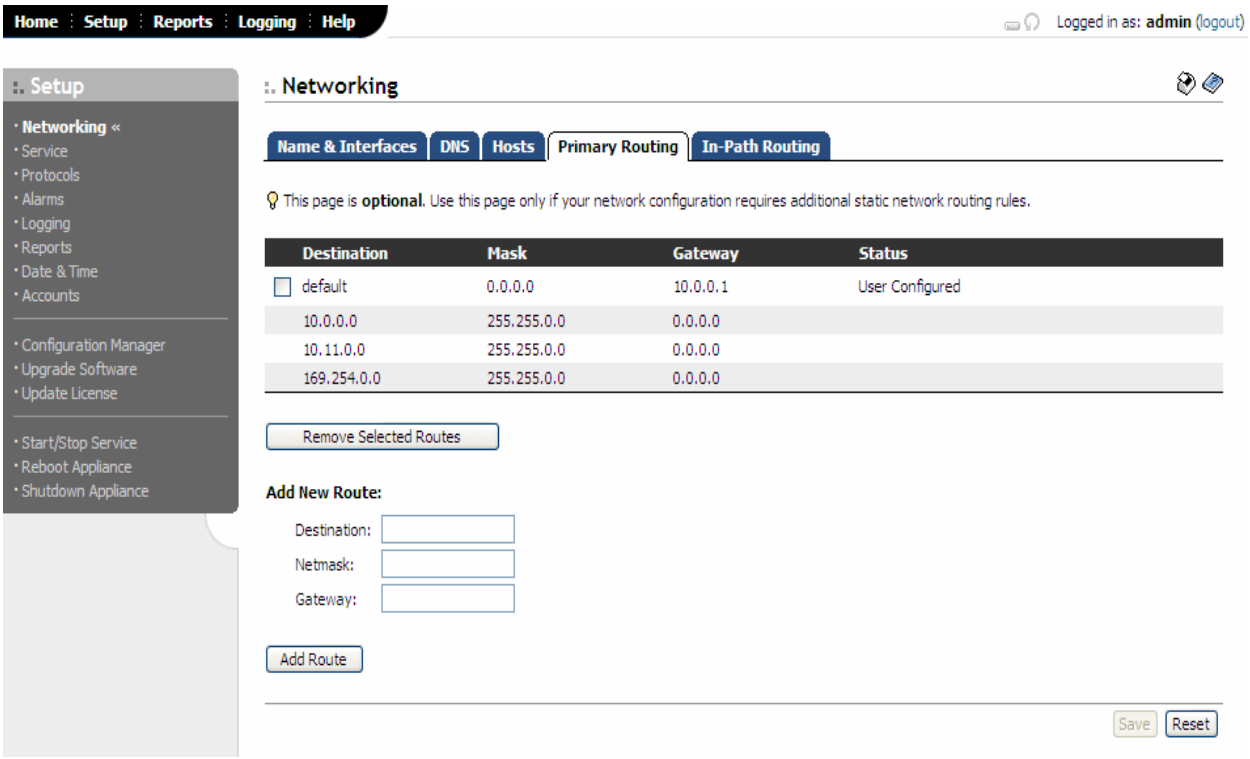
Setting Primary Network Routes

Optionally, configure static network routes in the Setup: Networking, Primary Routing page if your network configuration requires additional static network routing rules.

To set a primary network route

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click the Routing tab to display the Setup: Networking, Primary Routing page.

Figure 2-7. Setup: Networking, Primary Routing Page



3. Under Add New Route, type the destination IP address in the **Destination** text box.

4. Type the netmask in the **Netmask** text box.

5. Type the IP address for the gateway in the **Gateway** text box.

6. Click **Add Route** to add the route to the network routing list and apply your settings to the running configuration.

7. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove a primary route, click the check box next to the name and click **Remove Selected Routes**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

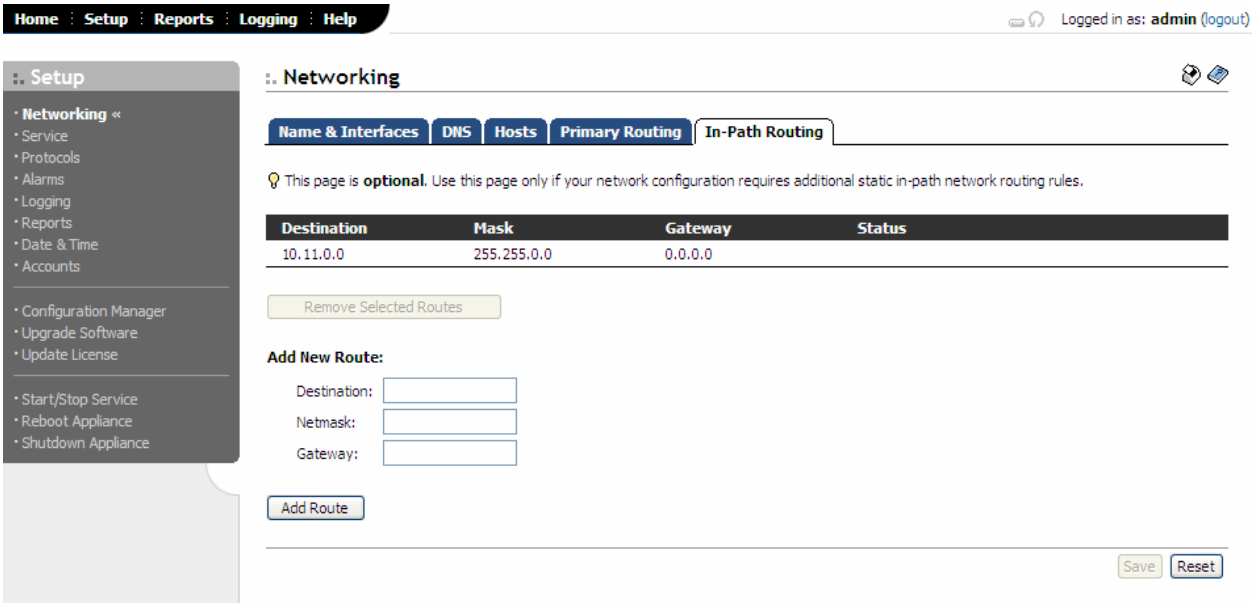
Setting In-Path Network Routes

Optionally, configure static in-path network routes in the Setup: Networking, In-Path Routing page. Configure this page only if your network configuration requires additional static in-path network routing rules.

To set a in-path network route

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click the Routing tab to display the Setup: Networking, In-Path Routing page.

Figure 2-8. Setup: Networking, In-Path Routing Page



3. Under Add New Route, type the destination IP address in the **Destination** text box.
4. Type the netmask in the **Netmask** text box.
5. Type the IP address for the gateway in the **Gateway** text box. This is your WAN gateway.
6. Click **Add Route** to add the route to the network routing list and apply your settings to the running configuration.
7. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove an in-path route, click the check box next to the name and click **Remove Selected Routes**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Configuring HP EFS WAN Accelerator Services

The following section describes how to configure HP EFS WAN Accelerator services. The services include: in-path, Virtual Local Area Network (VLAN) support, out-of-path, secure authentication, and failover support. You can also configure in-path rules, protocol properties, Quality of Service (QoS), and Differentiated Services Code Point (DSCP) levels. It includes the following sections:

Enabling Service Parameters

You set the following base service configuration parameters in the Setup: Service, Configuration page:

Enabling In-Path Support

During the initial setup of the HP EFS WAN Accelerator you had the option to enable and configure in-path support. Check or modify your settings in the Setup: Service, Configuration page.

In-path support is a network configuration in which the HP EFS WAN Accelerator is in the direct path of the server, the WAN, and the client. In-path support is transparent—the client and server are unaware of the HP EFS WAN Accelerator. For detailed information about in-path configurations, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

When you configure in-path support, you have the following options:

- **Enable External Traffic Redirection (Layer 4, PBR, WCCP)**. You enable external traffic redirection if you are using a Layer-4 switch to direct traffic to the WAN, Policy Based Routing (PBR), or Web Cache Communication Protocol (WCCP).

- **Layer 4 Switch**. You enable Layer 4 switch support when you have multiple HP EFS WAN Accelerators in your network to manage large bandwidth requirements. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
- **WCCP**. If your network design requires you to configure the HP EFS WAN Accelerator as an out-of-path device, you can use WCCP to configure the HP EFS WAN Accelerator out-of-path, yet redirect traffic through it to ensure it is optimized. For detailed information about WCCP deployments, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide* and the *HP EFS WAN Accelerator Command Line Interface Reference Manual*.
- **PBR**. Policy-Based Routing (PBR) allows you to define policies to route packets instead of relying on routing protocols. You enable PBR to redirect traffic that you want to optimize to an HP EFS WAN Accelerator that is configured as an out-of-path device. For detailed information about configuring the HP EFS WAN Accelerator in a PBR deployment, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide* and the *HP EFS WAN Accelerator Command Line Interface Reference Manual*.
- **Reset Existing Client Connections with Start Up.** If you enable the *kickoff* feature, connections that exist when the HP EFS WAN Accelerator service is started and restarted are disconnected. When the connections are retried they are optimized.

  Generally, connections are short lived and kickoff is not necessary. It is suitable for very challenging remote environments. For example, in an environment with 128 kbps and 1.5 seconds of latency, you might want to abort an HTTP download so that your traffic is optimized, whereas in a remote branch office with a T1 and 35 ms round-trip time, you would want connections to migrate to optimization gracefully, rather than risk interruption with kickoff.

NOTE: Do not enable kickoff for in-path HP EFS WAN Accelerators that use auto-discovery and if you do not have an HP EFS WAN Accelerator on the remote side of the network.

- **VLAN Tag ID**. The HP EFS WAN Accelerator supports VLAN 802.1q in an in-path configuration on a VLAN trunked link. The HP EFS WAN Accelerator automatically intercepts VLAN tagged connections when you specify the VLAN identification number for the interface and define in-path rules to apply to your VLANS in the Setup: Service In-Path Rules page.

  When you specify the VLAN Tag ID for the in-path interface, all packets originating from that HP EFS WAN Accelerator are tagged with that identification number. This is the VLAN tag that the HP EFS WAN Accelerator uses to communicate with other HP EFS WAN Accelerators in your network. The VLAN Tag ID might be the same value or a different value than the VLAN tag used on the client. A zero specifies non-tagged (or native) VLAN.

  When the HP EFS WAN Accelerator communicates with a client or a server it uses the same VLAN tag as the client or the server. If the HP EFS WAN Accelerator cannot determine which VLAN the client or server is in, it uses its own VLAN until it is able to determine that information.

IMPORTANT: You must also set VLAN Tag IDs in the Setup: Services, In-Path Rules page. You can configure in-path rules to apply to all VLANS or to a specific VLAN. By default, rules apply to all VLAN values unless you specify a particular VLAN Tag ID. Pass-through traffic maintains any pre-existing VLAN tagging between the LAN and WAN interfaces. For detailed information about setting VLAN IDs for in-path rules, see the "Setting In-Path Rules" on page 46.

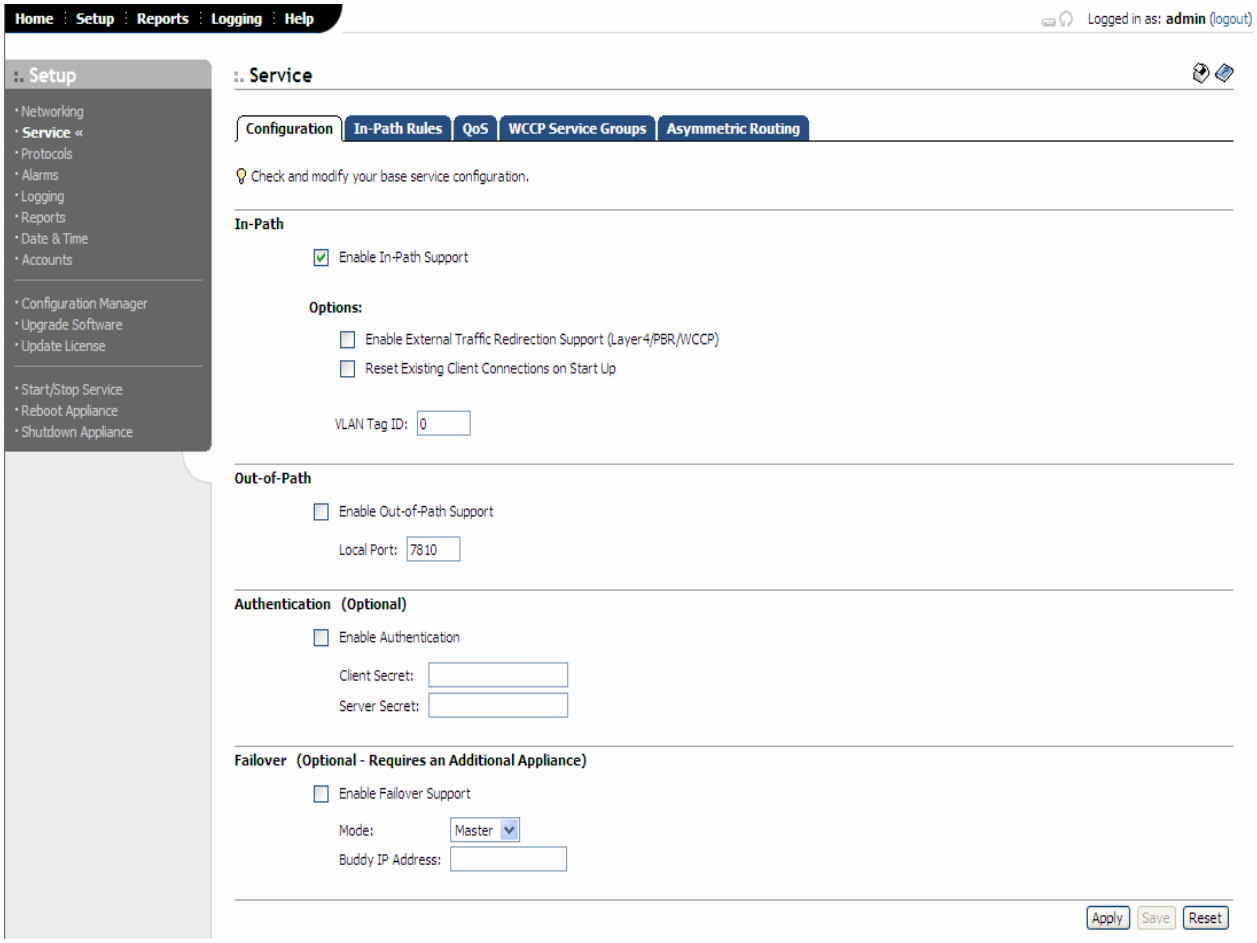
IMPORTANT: The HP EFS WAN Accelerator does not support the Cisco InterSwitch Link (ISL) protocol.

To enable in-path support

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

2. Click Service in the left menu to display the Setup: Service, Configuration page.

Figure 2-9. Setup: Service, Configuration Page



3. Under In-Path, click **Enable In-Path Support** to enable optimization on traffic that is in the direct path of the client, server, and HP EFS WAN Accelerator.

4. Under options, click **Enable External Traffic Redirection Support (Layer 4, PBR, WCCP)** if you are using a Layer 4 switch, PBR, or WCCP to redirect traffic.

5. Click **Reset Existing Client Connections with Start Up** to enable optimization on your client connections each time you log in. Generally, connections are short lived and this setting is not necessary. Set kickoff if you have a very challenging remote environment.

6. Type the VLAN identification number in the **VLAN Tag ID** text box that you want to use to communicate between HP EFS WAN Accelerators in your network.

IMPORTANT: You must also set in-path rules to apply to your VLANS in the "Setting In-Path Rules" on page 46.

7. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it to memory.)
8. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Enabling Out-of-Path Support

Optionally, you can enable out-of-path support in the Setup: Service, Configuration page. An out-of-path device is a device that is not in the direct path of packets to a server.

For example, an out-of-path configuration is suitable for data centers because applications connect to servers at this site. (Some data centers might not be suitable for out-of-path configurations because of the applications that connect from the data center such as backup applications.)

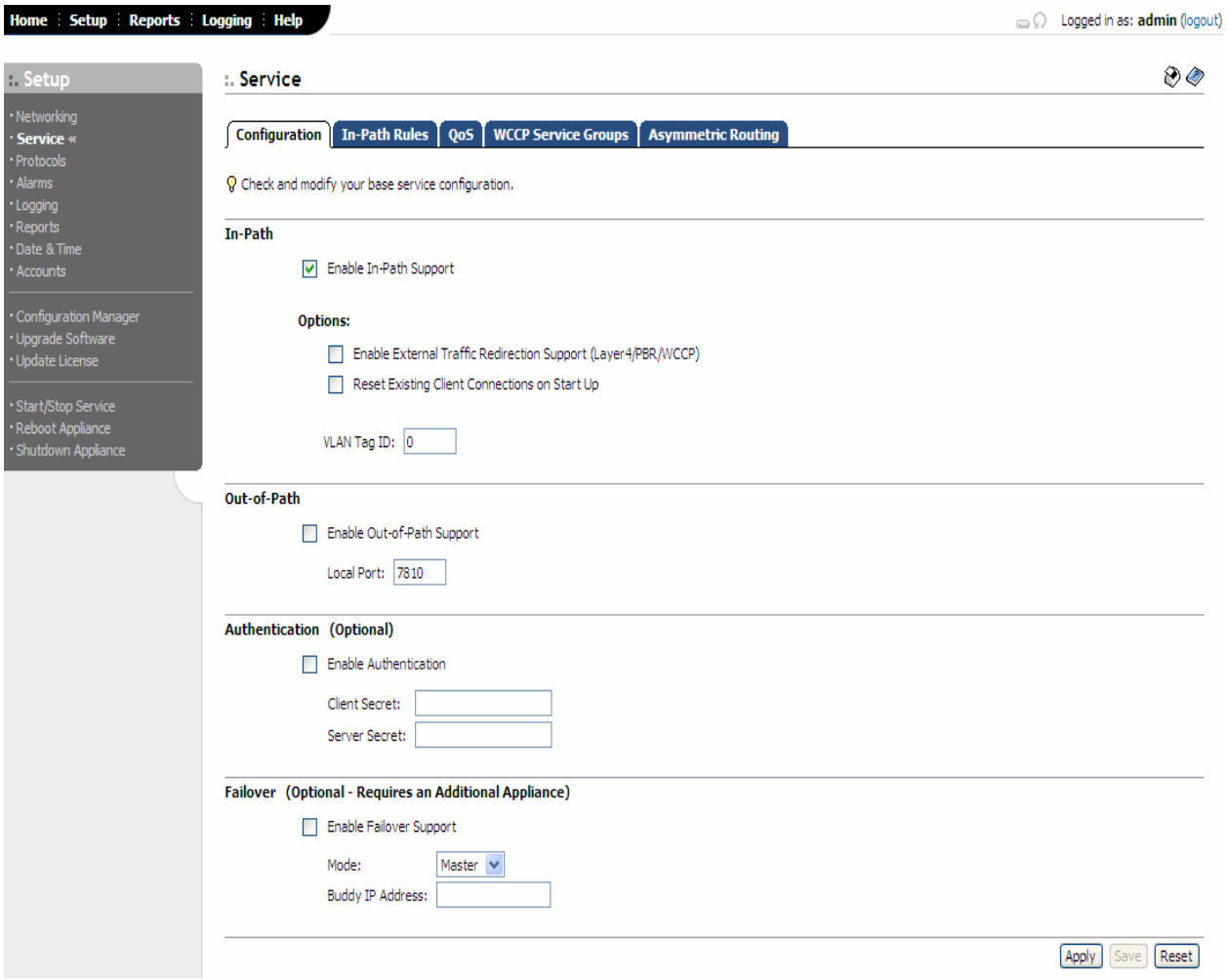
For detailed information about out-of-path configurations, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

NOTE: If you have an out-of-path configuration with failover support, you must specify the master and backup HP EFS WAN Accelerators in the Setup: Service, In-Path Rules, Fixed-Target page. For detailed information, see "Setting In-Path Rules" on page 46.

To enable out-of path support

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Service in the left menu to display the Setup: Service, Configuration page.

Figure 2-10. Setup: Service, Configuration Page



3. Under Out-of-Path, click **Enable Out-of-Path Support** and type a port number in the **Local Port** text box.
4. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)
5. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Enabling HP EFS WAN Accelerator Secure Authentication

Optionally, you can configure authentication for HP EFS WAN Accelerators to ensure that connections between appliances are secure. The HP EFS WAN Accelerators use shared secrets to form responses to authentication challenges. The secrets are strings of data that HP EFS WAN Accelerators on both sides of the network share, but do not actually transfer over the network.

You specify the following types of secrets:

- **Client Secret (Secret1)**. Authenticates peers that are connected to your HP EFS WAN Accelerator.
- **Server Secret (Secret2)**. Authenticates peers that your HP EFS WAN Accelerator is connected to.

You can define secrets to be the same on all participating HP EFS WAN Accelerators and enable them for the peers that you want to authenticate:

- Appliance1: secret1 (client) = foo, secret2 (server) = bar, enable = false
- Appliance2: secret1 (client) = foo, secret2 (server) = bar, enable = true
- Appliance3: secret1 (client) = foo, secret2 (server) = bar, enable = true

Appliance1 is authenticated when connecting to Appliance2, but not when Appliance3 connects to it. Typically, you will authenticate all the HP EFS WAN Accelerators or none.

NOTE: You cannot enable authentication if either of the secrets are blank.

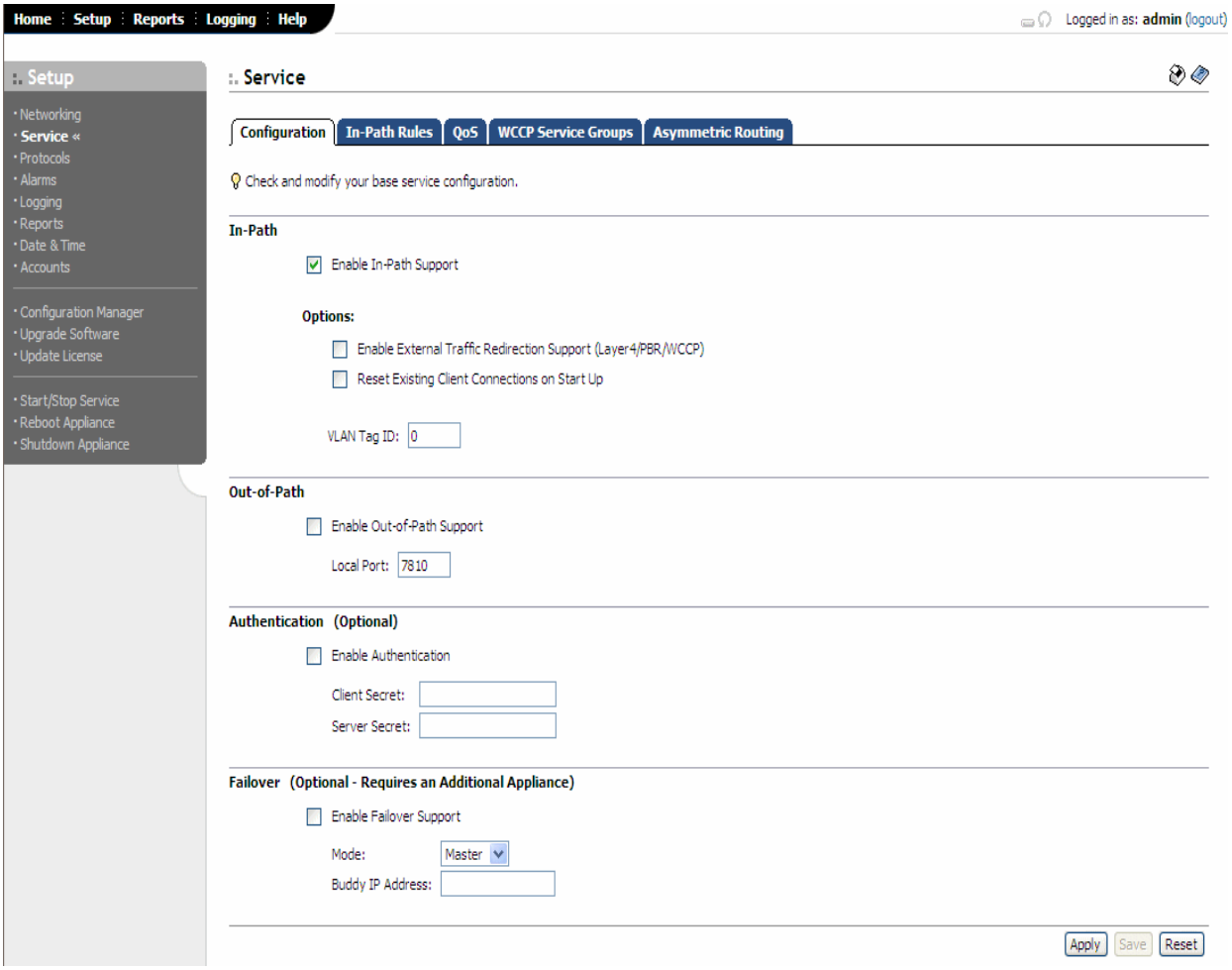
For optimum security, the secrets must be at least 16 bytes, although this is not necessary for operation. The two secrets can be identical, but this decreases security.

Secrets must be shared on both sides of the system. For example, suppose you need to authenticate on the server-side HP EFS WAN Accelerator, but you do not need to on the client-side HP EFS WAN Accelerator. You must enable authentication and specify secrets on the server-side HP EFS WAN Accelerator. On the client-side HP EFS WAN Accelerator, you do not enable authentication, but you do specify the secrets.

To enable HP EFS WAN Accelerator authentication

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Service in the left menu to display the Setup: Service, Configuration page.

Figure 2-11. Setup: Service, Configuration Page



3. Under Authentication, click **Enable Authentication** to enable authentication between HP EFS WAN Accelerators.

TIP: If you simply need to share secrets between two HP EFS WAN Accelerators do not click **Enable Authentication**.

---

4. Type a secret for the client-side HP EFS WAN Accelerator in the **Client Secret** text box.

5. Type a secret for the server-side HP EFS WAN Accelerator in the **Server Secret** text box.

NOTE: To enable authentication, both secrets must be specified.

6. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)

7. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Enabling Failover Support

Optionally, you can set failover support in the Setup: Service, Configuration page. Failover support ensures continued optimization if there is a failure with one of the HP EFS WAN Accelerators. If the *master* HP EFS WAN Accelerator fails, the traffic is automatically processed by the *backup* HP EFS WAN Accelerator using the *buddy* IP address.

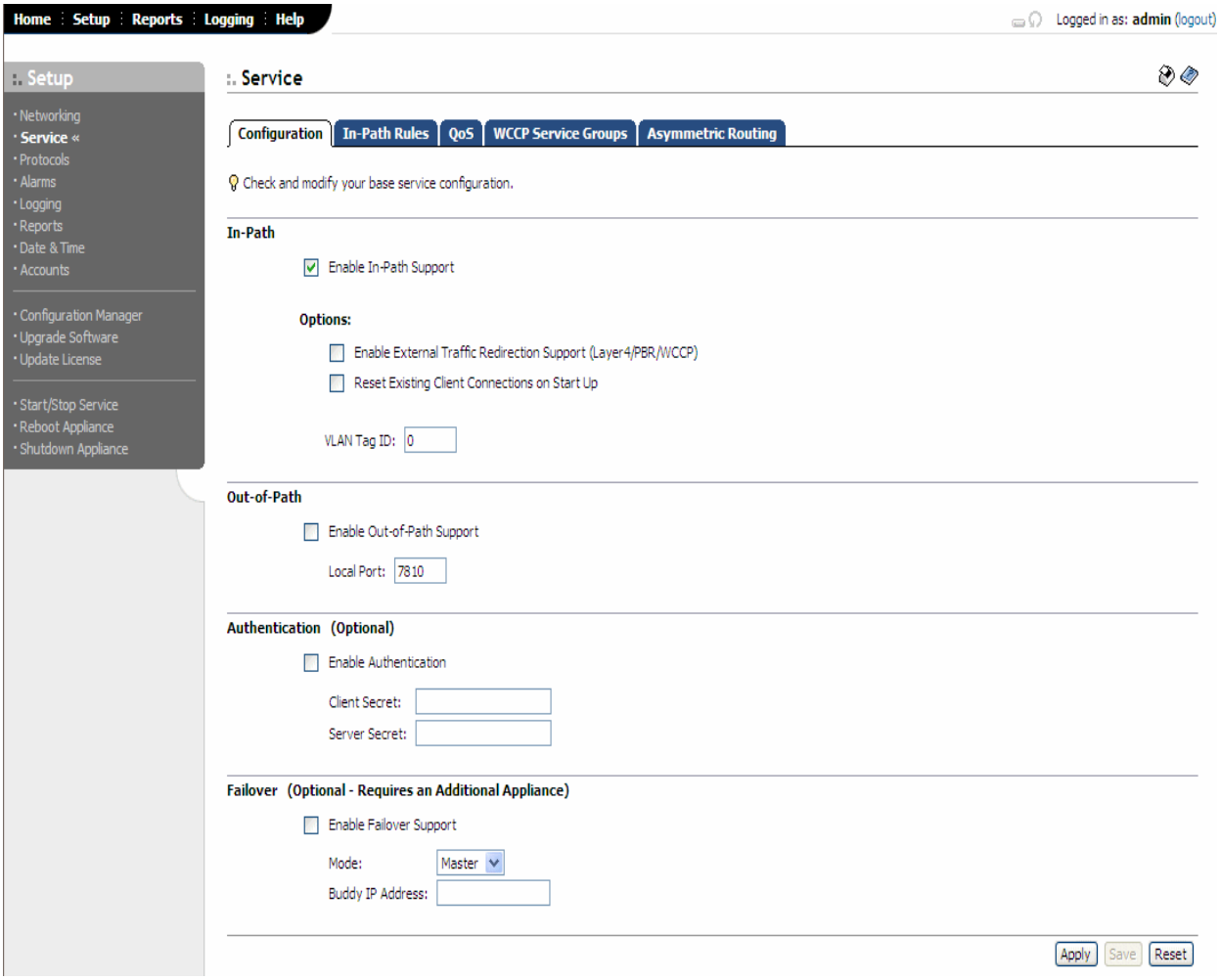
NOTE: If you have an out-of-path configuration with failover support, you must specify the master and backup HP EFS WAN Accelerators in the Setup: Service, In-Path Rules, Fixed-Target page. For detailed information, see "Setting In-Path Rules" on page 46.

To set the failover appliance

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

2. Click Service in the left menu to display the Setup: Service, Configuration page.

Figure 2-12. Setup: Service, Configuration Page



3. Under Failover, click **Enable Failover Support** to enable a failover HP EFS WAN Accelerator.

4. Select **Master** or **Backup** from the **Mode** drop-down list. A master appliance is the primary HP EFS WAN Accelerator; the backup appliance is the HP EFS WAN Accelerator that automatically forwards traffic if the master appliance fails.

5. Type the IP address for the master or backup HP EFS WAN Accelerator in the **Buddy IP Address** text box.

6. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)

7. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Setting In-Path Rules

You set in-path configuration rules in the Setup: Service, In-Path Rules page. An in-path rule defines the policies for intercepting traffic for optimization. By default, the HP EFS WAN Accelerator automatically intercepts and optimizes traffic on all IP addresses (**0.0.0.0**) and ports (**all**). Defining in-path rules modifies the default setting.

You can also specify the VLAN identification number so that the connections for a particular VLAN are intercepted and optimized or passed-through unoptimized in the Setup: Service, In-Path Rules page.

In-Path Rules

You can have the following in-path rules:

- **Auto-Discovery**. Auto-discovery rules automatically find the HP EFS WAN Accelerators between this appliance and the server for which the packet is destined. For detailed information about in-path configurations, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.
- **Fixed Target**. Fixed target rules directly specify out-of-path HP EFS WAN Accelerators near the target server. Determine which servers you would like a particular HP EFS WAN Accelerator to optimize (and, optionally, which ports), and add rules to specify the network of servers, ports, and out-of-path HP EFS WAN Accelerators to use. For detailed information about out-of-path configurations, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

  (If you have an out-of-path configuration with failover support, you specify the master and backup HP EFS WAN Accelerators in the Setup: Service, In-Path Rules page.)
- **Pass Through**. Pass through rules identify traffic that is passed through the network unoptimized.

The HP EFS WAN Accelerator applies rules in numerical order starting with rule 1. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.

It is important to plan your in-path rules so that your network conditions are met. Typically, most rules are listed in the following order:

1. **Pass through**. List the exceptions to optimize first.
2. **Fixed target**. List any fixed targets next.
3. **Auto-discovery**. Apply the default rule: optimize all remaining traffic. (The default auto-discovery rule is listed automatically.)

VLAN IDs for In-Path Rules

You can set VLAN tag IDs in the Setup: Service, In-Path Rules page to optimize all VLANs or specific VLANs. Pass-through traffic maintains any pre-existing VLAN tagging between the LAN and WAN interfaces.

Passing-Through Traffic on Secure and Interactive Ports

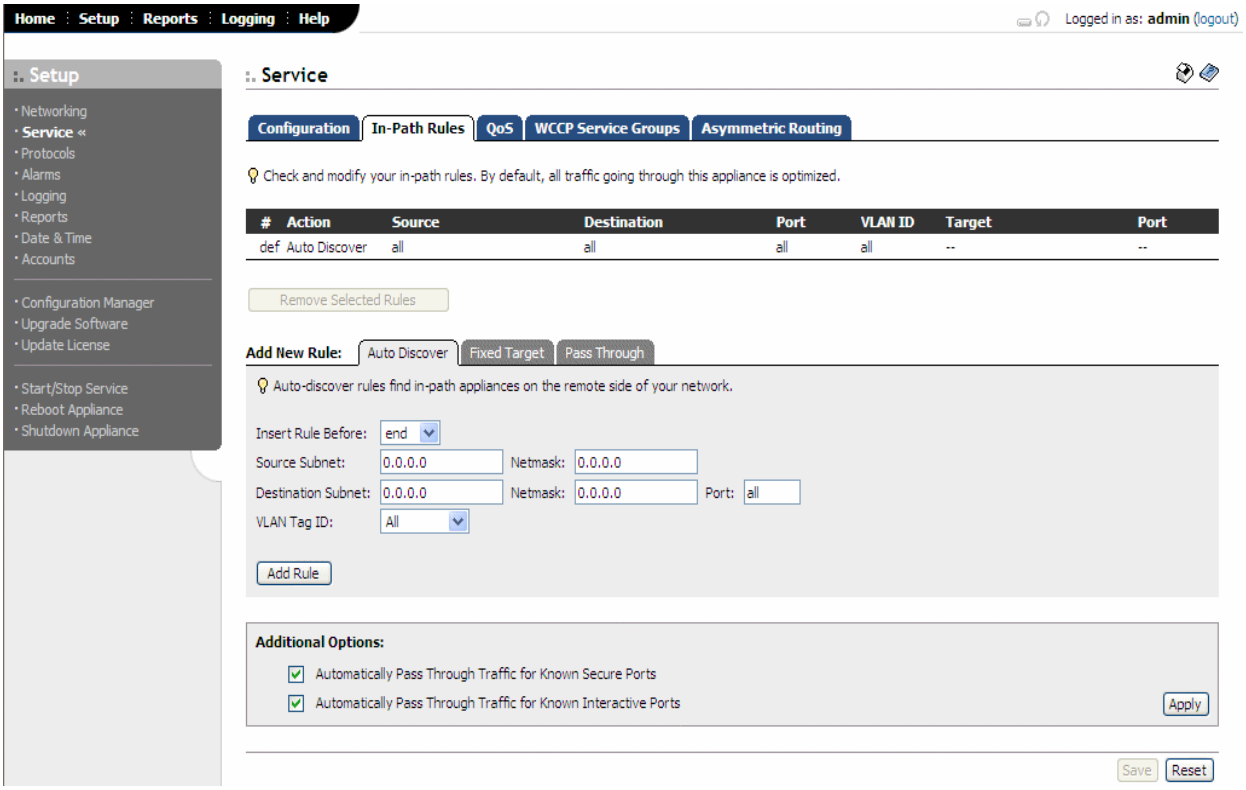
You can also automatically forward traffic on secure and interactive ports in the Setup: Service In-Path Rules page:

- **Pass-Through Traffic for Known Secure Ports**. Automatically pass through traffic on commonly secure ports (for example, **ssh**, **https**, and **smtps**). For a list of ports that are automatically forwarded, see "Secure Ports Automatically Forwarded by the HP EFS WAN Accelerator" on page 120.
- **Pass-Through Traffic for Known Interactive Ports**. Automatically pass through traffic on interactive ports (for example, Telnet, TCP ECHO, remote logging, and shell). For a list of interactive ports that are automatically forwarded, see "Interactive Ports Automatically Forwarded by the HP EFS WAN Accelerator" on page 120.

To set an in-path, auto-discovery rule

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Service in the left menu to display the Setup: Service, Configuration page.
3. Click the In-Path Rules tab to display the Setup: Service, In-Path Rules, Auto-Discovery page.

Figure 2-13. Setup: Service, In-Path Rules, Auto-Discovery Page



4. Under Add New Rule, select **start**, **end**, or a **rule number** from the **Insert Rule Before** drop-down list to insert a rule before the rule specified in the Rules list.

5. Type the IP address and netmask for the source subnet in the **Source Subnet** and **Netmask** text boxes.

6. Type the IP address, netmask, and port for the destination subnet in the **Destination Subnet, Netmask,** and **Port** text boxes. By default, the HP EFS WAN Accelerator applies the rule to all ports.

7. Select the VLAN identification number from the **VLAN Tag ID** drop-down list box. **All** specifies the rule applies to all VLANS; zero (**0**) specifies the rule applies to non-tagged connections.

8. Click **Add Rule** to apply the rule to the running configuration.

9. Under Additional Options, click **Pass Through Traffic for Known Secure Ports** and **Apply** if you want to forward traffic on secure ports. For example, **ssh**, **https**, and **smtps**.

10. Click **Pass Through Traffic for Known Interactive Ports** and **Apply** if you want to forward traffic on interactive ports. For example, Telnet, TCP ECHO, remote logging, and shell.

11. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove a rule, click the check box next to the name and click **Remove Selected Rules**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To move a rule, select the rule you want to move from the **Move Rule** drop-down list, select the location where you want to move it to from the **to** drop-down list, and click **Move Rule**.

To set a fixed target rule

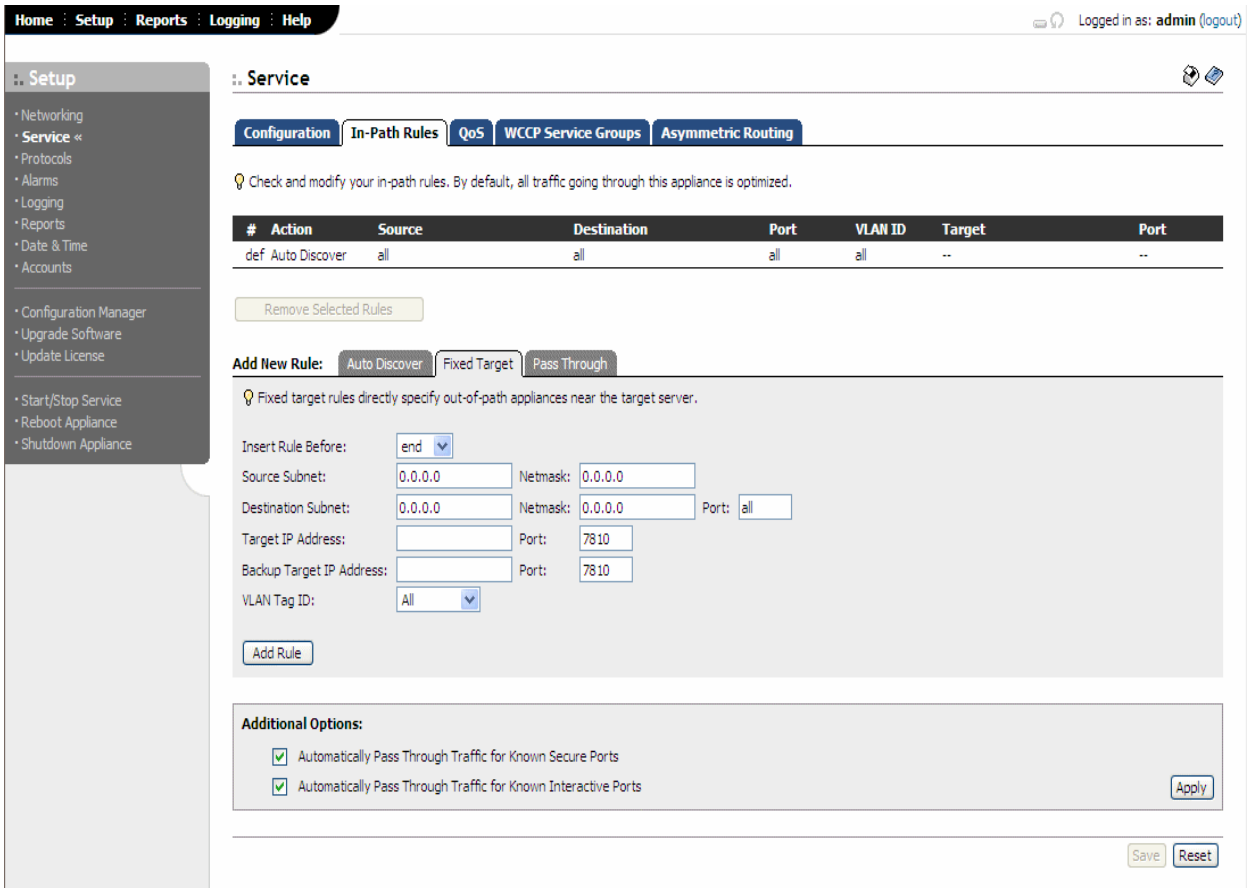
1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

2. Click Service in the left menu to display the Setup: Service, Configuration page.

3. Click the In-Path Rules tab to display the Setup: Service, In-Path Rules, Auto-Discovery page.

4. Click the Fixed Target tab to display the Setup: Service, In-Path Rules, Fixed Target page.

Figure 2-14. Setup: Service, In Path Rules, Fixed Target Page



5. Under Add New Rule, select **start**, **end**, or a **rule number** from the **Insert Rule Before** drop-down list to insert a rule before the rule specified in the Rules list.

6. Type the IP address and netmask for the source subnet in the **Source Subnet** and **Netmask** text boxes.

7. Optionally, type the IP address, netmask, and port for the destination subnet in the **Destination Subnet**, **Netmask**, and **Port** text boxes.

8. Type the IP address and port number for the HP EFS WAN Accelerator that is the peer in the **Target IP Address** and **Port** text boxes. The IP address must be the Primary Port IP address on the target HP EFS WAN Accelerator. The default port is **7810**.

9. If you have a backup, out-of-path, HP EFS WAN Accelerator in your system (that is, failover support), type the IP address and port for the backup appliance in the **Backup Target IP Address** and **Port** text boxes. The default port is **7810**.

10. Select the VLAN identification number from the **VLAN Tag ID** drop-down list box. **All** specifies the rule applies to all VLANS; zero (**0**) specifies the rule applies to non-tagged connections.

11. Click **Add Rule** to apply the rule to the running configuration.

12. Under Additional Options, click **Pass Through Traffic for Known Secure Ports** and **Apply** if you want to forward traffic on secure ports. For example, **ssh**, **https**, and **smtps**.

13. Click **Pass Through Traffic for Known Interactive Ports** and **Apply** if you want to forward traffic on interactive ports. For example, Telnet, TCP ECHO, remote logging, and shell.

14. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove a rule, click the check box next to the name and click **Remove Selected Rules**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To move a rule, select the rule you want to move from the **Move Rule** drop-down list, select the location where you want to move it from the **to** drop-down list, and click **Move Rule**.

To set a pass-through rule

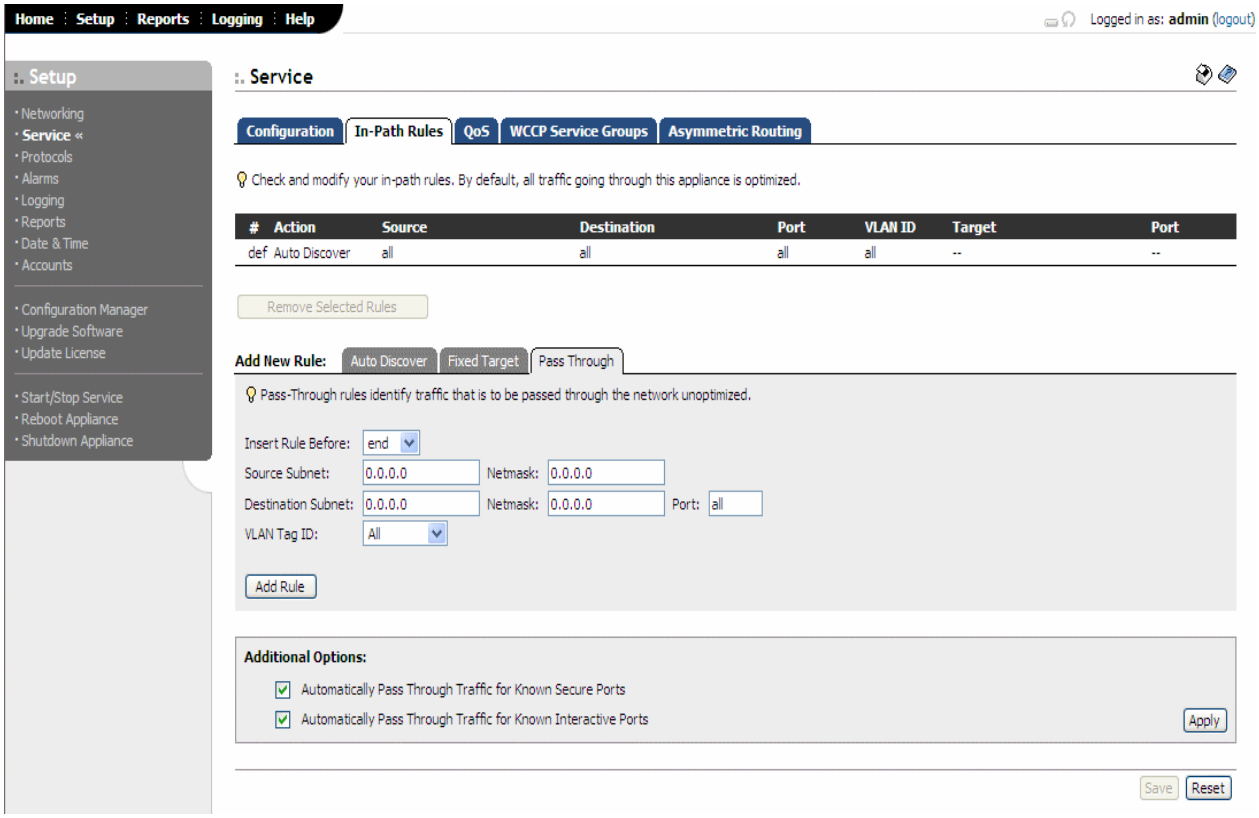
1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

2. Click Service in the left menu to display the Setup: Service, Configuration page.

3. Click the In-Path Rules tab to display the Setup: Service, In-Path Rules, Auto-Discovery page.

4. Click the Pass Through tab to display the Setup: Service, In-Path Rules, Pass Through page.

Figure 2-15. Setup: Service, In-Path Rules, Pass Through Page



5. Under Add New Rule, select **start**, **end**, or a rule number from the **Insert Rule Before** drop-down list to insert a rule before the rule specified in the Rules list.

6. Optionally, type the IP address and netmask for the source subnet in the **Source Subnet** and **Netmask** text boxes.

7. Type the IP address, netmask, and port for the destination subnet in the **Destination Subnet**, **Netmask**, and **Port** text boxes. By default, the HP EFS WAN Accelerator applies the rule to all ports.

8. Select the VLAN identification number from the **VLAN Tag ID** drop-down list box. **All** specifies the rule applies to all VLANS; zero (**0**) specifies the rule applies to non-tagged connections.

9. Click **Add Rule** to apply the rule to the running configuration.

10. Under Additional Options, click **Pass Through Traffic for Known Secure Ports** and **Apply** if you want to forward traffic on secure ports. For example, **ssh**, **https**, and **smtps**.

11. Click **Pass Through Traffic for Known Interactive Ports** and **Apply** if you want to forward traffic on interactive ports. For example, Telnet, TCP ECHO, remote logging, and shell.

12. Click **Add Rule** to apply the rule to the running configuration.

13. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove a rule, click the check box next to the name and click **Remove Selected Rules**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To move a rule, select the rule you want to move from the **Move Rule** drop-down list, select the location where you want to move it to from the **to** drop-down list, and click **Move Rule**.

Setting QoS Levels

Optionally, you can set QoS levels in the Setup: Service, QoS page. The QoS feature allows you to map a service port to a Differentiated Services Codepoint (DSCP) level. The DSCP level corresponds to the DiffServ DSCP field in the IP packets header.

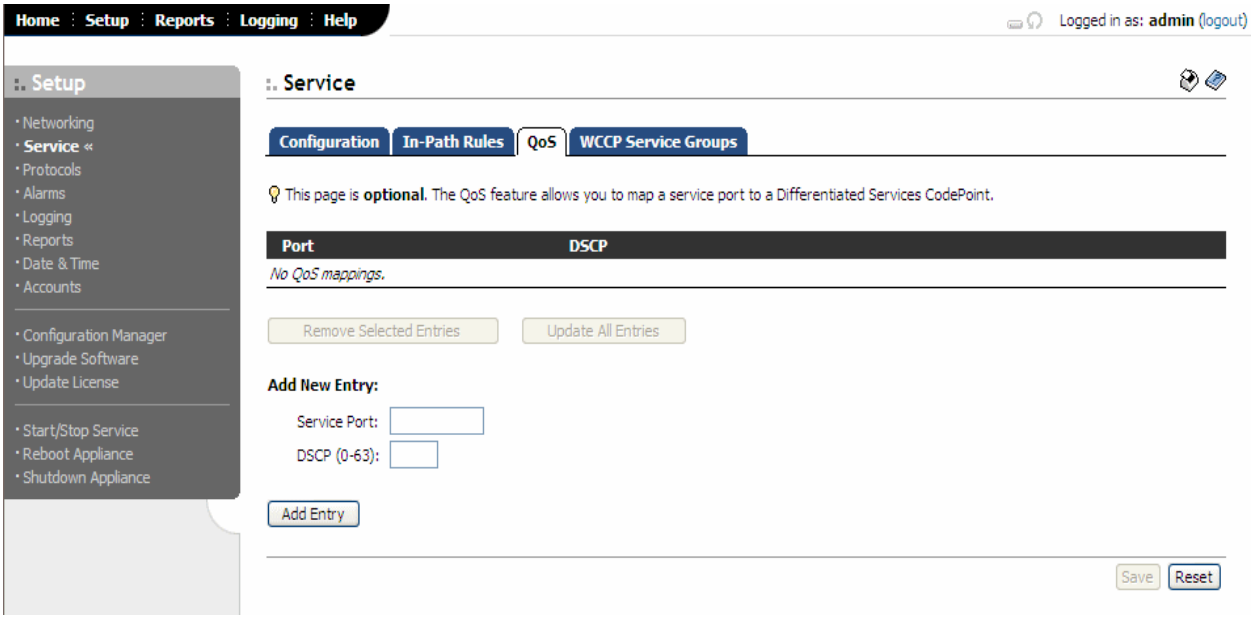
After you map a service port and a DSCP level, every packet using that service port has the DSCP field set to that value in the forward and backward direction. On the WAN HP EFS WAN Accelerator, you can configure a network router or a traffic shaper to prioritize packets according to the value in the DSCP field before they are sent over the WAN.

IMPORTANT: If you have already defined a DSCP level and you do not define one in the Management Console, the HP EFS WAN Accelerator uses the existing DSCP level for the connection between the appliances. If you define a DSCP level in the Management Console, the HP EFS WAN Accelerator overrides the existing DSCP level and the value that you defined is applied.

To set a QoS level

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Service in the left menu to display the Setup: Service, Configuration page.
3. Click the QoS tab to display the Setup: Service, QoS page.

Figure 2-16. Setup: Service, QoS Page



4. Under Add New Entry, type the port number on which you want to enforce QoS in the **Service Port** text box.
5. Type a number for the DSCP level you want to enforce in the **DSCP** text box.
6. Click **Add Entry** to apply your settings to the running configuration.
7. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove a QoS service, click the check box next to the name and click **Remove Selected Entries**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To edit the QoS entries, click **Update All Entries**.

Setting WCCP Service Groups

Optionally, you can set WCCP service groups in the Setup: Service, WCCP Service Groups page. WCCP enables you to redirect traffic through the HP EFS WAN Accelerator that is configured as an out-of-path device.

TIP: You can also use the HP EFS WAN Accelerator CLI to configure WCCP service groups. For detailed configuration information (including configuring the WCCP router), see the *HP EFS WAN Accelerator Command Line Interface Reference Manual*.

NOTE: The following section assumes you are familiar with WCCP. For detailed information about WCCP, see the Cisco documentation Web site at **http://www.cisco.com/univercd/home/home.htm**.

To enable WCCP, the HP EFS WAN Accelerator must join a service group at the router. A service group is a group of routers and HP EFS WAN Accelerators which define the traffic to redirect, and the routers and HP EFS WAN Accelerators the traffic goes through.

WCCP Parameters

The following table summarizes the parameters you set for WCCP support.

Field	Description
Service Group ID	The service group ID is a number from 0 to 255 identifying a particular service group. The service group ID is the number that is set on the router. A value of 0 specifies the standard **http** service group.
Router IP	The router IP is multicast group IP address or a unicast router IP address. A total of 32 routers can be specified. (After you have created a new service group, click the service group name to add additional routers. A total of 32 routers can be specified.)
Password	Optionally, you can assign a password to the HP EFS WAN Accelerator. This password must be the same as the password on the router. (WCCP requires that all routers in a service group have the same password.) Passwords are limited to 8 characters.

Field	Description
Priority	If a connection matches multiple service groups on a router, the router chooses the service group with the highest priority. The default value is **200**. The range is **0-255**.
Weight	The weight determines how often the traffic is redirected to a particular HP EFS WAN Accelerator. A higher weight redirects more traffic to that HP EFS WAN Accelerator. The ratio of traffic redirected to an HP EFS WAN Accelerator is equal to its weight divided by the sum of the weights of all the HP EFS WAN Accelerators in the same service group. For example, if there are 2 HP EFS WAN Accelerators in a service group and one has a weight of **100** and the other has a weight of **200**, the one with the weight **100** receives 1/3 of the traffic and the other receives 2/3 of the traffic. The range is **0-65535**. The default value corresponds to the HP EFS WAN Accelerator model (for example, for the Model 5000 the default value is **5000**; for the Model 2000 the default value is **2000**).
Encapsulation Scheme	Specifies the traffic forwarding and redirection scheme: Generic Routing Encapsulation (**gre**) or Layer-2 (**l2**) redirection. The **either** value uses Layer-2 first—if Layer-2 is not supported, **gre** is tried.
Version	Optionally, you can enable WCCP, version 2 support.
Multicast Time to Live (TTL)	If you enable WCCP, version 2 support, you can specify the TTL boundary for the WCCP protocol packets. The default value is **5** (global for all service groups).
Source IP Hash, Source Port Hash, Destination IP Hash, or Destination Port Hash	Specifies the fields the router hashes on. You set the source and destination IP and port hash fields after you have configured WCCP service groups. For detailed information, see "To edit a WCCP service group" on page 58.
Source, **Destination**	If the source or destination port is set, the router only redirects TCP traffic with the same source or destination port that is specified in the Ports list. You set the source and destination ports after you have configured WCCP service groups. For detailed information, see "To edit a WCCP service group" on page 58

Enabling Failover Support for WCCP

To enable failover support with WCCP groups, define the service group weight to be **0** on the backup HP EFS WAN Accelerator. If one HP EFS WAN Accelerator has a weight **0**, but another one has a non-zero weight, the HP EFS WAN Accelerator with weight **0** does not receive any redirected traffic. If all the HP EFS WAN Accelerators have a weight **0**, the traffic is redirected equally among them.

For detailed information about enabling failover (backup) support, see "Enabling Failover Support" on page 44.

Modifying Service Groups Settings and Adding Source and Destination Ports

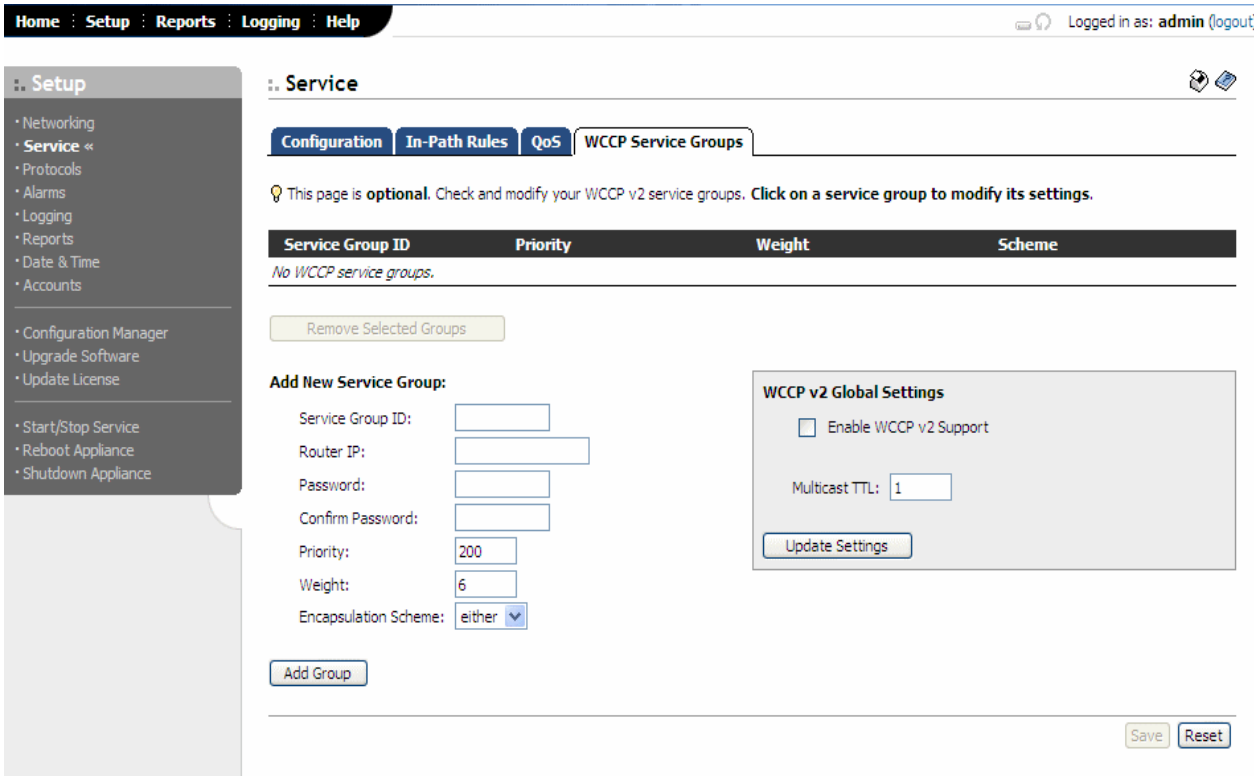
After you have added a service group, you can modify service group settings, add additional routers to a service group, and set flags for source and destination ports to redirect traffic (that is, the hash table settings). If the source or destination flags are set, the router redirects the TCP traffic that matches the source or destination ports specified.

NOTE: For detailed information about hash table settings for WCCP, see the Cisco documentation Web site at **http://www.cisco.com/univercd/home/home.htm**.

To set a WCCP service group

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Service in the left menu to display the Setup: Service, Configuration page.
3. Click the WCCP Service Groups tab to display the Setup: Service, WCCP Service Groups page.

Figure 2-17. Setup: Service, WCCP Service Groups Page



4. Under Add New Service Group, type the service group identification number in the **Service Group ID** text box.

5. Type the IP address for the router in the **Router IP** text box.

TIP: After you have created a new service group, click the service group name to add additional routers. A total of 32 routers can be specified.

---

6. Optionally, type the service group password in the **Password** text box. Retype the service group password in the **Confirm Password** text box.

7. Optionally, modify the priority number in the **Priority** text box to assign a priority to the service group. The default value is **200**. The range is **0-255**.

8. Optionally, modify the weight in the **Weight** text box to assign a weight to the HP EFS WAN Accelerator. The range is **0-65535**.

9. Select **either**, **gre,** or **l2** from the **Encapsulation Scheme** drop-down list to redirect packets using Generic Routing Encapsulation (**gre**) or Layer-2 (**l2**) redirection. The **either** value tries Layer-2 first, then **gre**.

10. Click **Add Group** to apply your settings to the running configuration.

11. Under WCCP v2 Global Settings, click **Enable WCCP v2 Support** to enable WCCP, version 2 support.

12. Optionally, modify the number in the **Multicast TTL** text box to set a TTL boundary for the WCCP protocol packets. The default value is **5** (global for all service groups).

13. Click **Update Settings** to apply your settings to the running configuration.

14. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

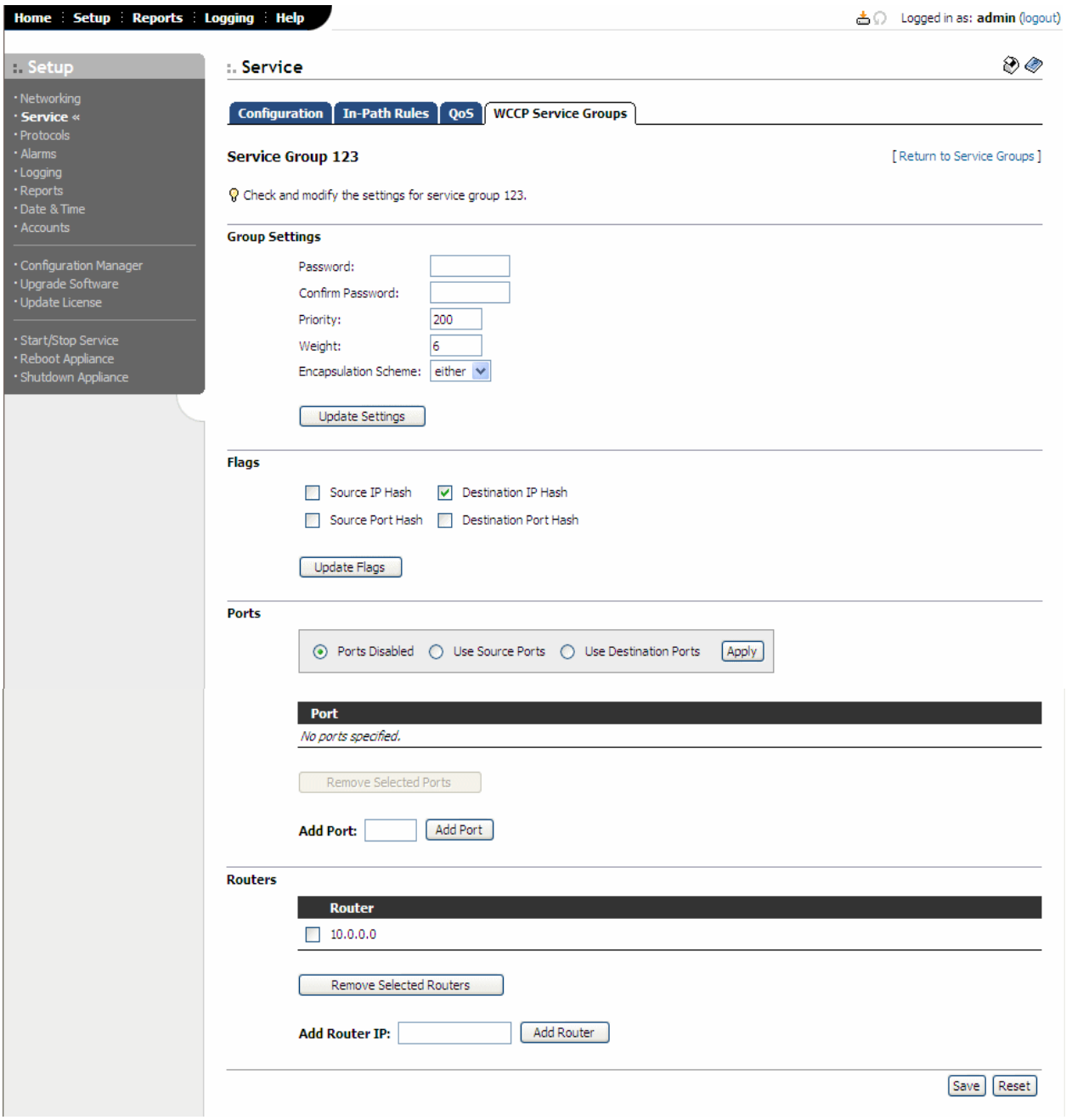
TIP: Click the service group you want to modify to display the Setup: Service, WCCP Groups page.

TIP: To remove a service group, click the check box next to the name and click **Remove Selected Groups**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

To edit a WCCP service group

1. Click the service group you want to modify to display the Setup: Service, WCCP Groups page.

Figure 2-18. Setup: Service, WCCP Groups Page



2. Optionally, under Group Settings, highlight and delete the old password in the **Password** and **Confirm Password** text boxes.

3. Type a new service group password in the **Password** and **Confirm Password** text boxes. The password is limited to 8 characters.

4. Optionally, modify the priority number in the **Priority** text box to assign a priority to the service group. The default value is **200**. The range is **0-255**.

5. Optionally, modify the weight in the **Weight** text box to assign a redirection weight to the HP EFS WAN Accelerator. The range is **0-65535**.

6. Select **either**, **gre** or **l2** from the **Encapsulation Scheme** drop-down list to redirect packets using Generic Routing Encapsulation (**gre**) or Layer-2 (**l2**) redirection. The **either** value uses Layer-2 first, then **gre**.

7. Click **Update Settings** to apply your new settings to the running configuration.

8. Under Flags, click **Source IP Hash**, **Source Port Hash**, **Destination IP Hash**, or **Destination Port Hash** to define the fields the router hashes on.

9. Under Ports, click **Source** or **Destination**. If a source or destination is specified, the router redirects only that TCP traffic with the same source or destination ports specified in the Ports list.

10. If you set a source or destination port, under Ports, type the port number in the **Port Number** text box and click **Add Port**. You can add 7 ports.

NOTE: For detailed information about hash table settings for WCCP, see the Cisco documentation Web site at **http://www.cisco.com/univercd/home/home.htm**.

---

11. Under Routers, type the IP address for the router in the **Add Router IP** text box and click **Add Router** to add additional routers to the service group.

12. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove ports, click the check box next to the port name and click **Remove Selected Ports**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove routers, click the check box next to the router IP address and click **Remove Selected Router**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Setting Protocol Properties

The following section describes how you set Common Internet File System (CIFS) write-through, CIFS transparent pre-population, Mail API (MAPI) transparent prepopulation, and a Name Service Provider Interface (NSPI) port. It contains the following sections:

Enabling CIFS Write-Through and Transparent Prepopulation

You enable the following CIFS features on the Setup: Protocols, CIFS page:

- **Disable CIFS Write Optimization (write-through)**. You disable CIFS write optimization only if you have applications that do not support write-through in the network. If you disable write-through, the HP EFS WAN Accelerator still provides optimization for CIFS reads and for other protocols, but you might experience a slight decrease in overall optimization.

  Most applications are written to operate safely with write-through because CIFS allows you to specify write-through on each write operation. However, if you have an application that does not support write-through in the network, you must disable it in the HP EFS WAN Accelerator.

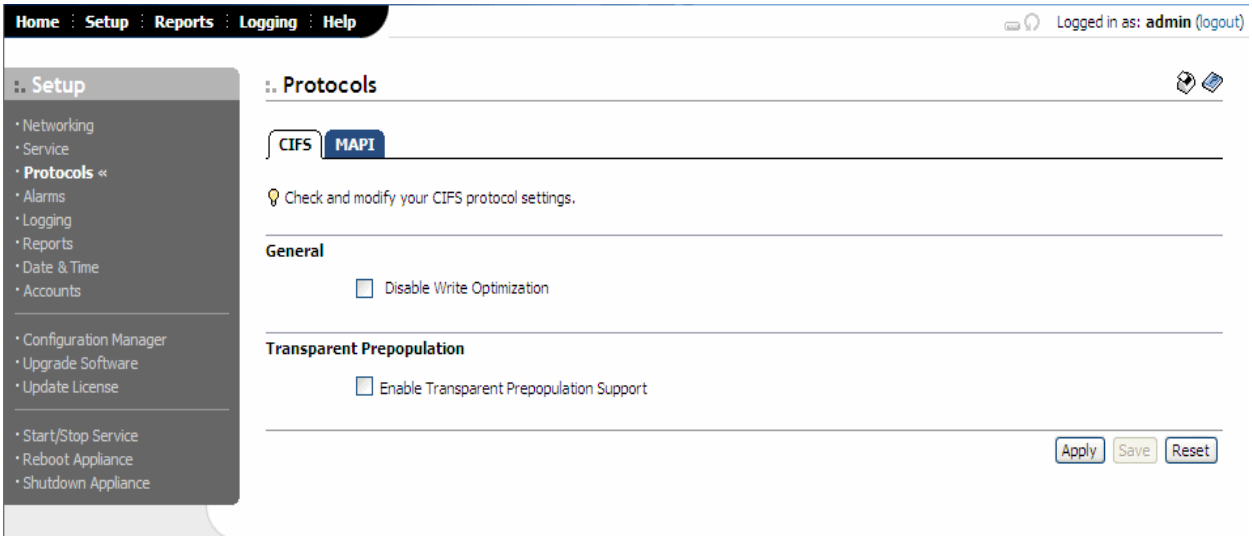
  If you do not disable write-through, the HP EFS WAN Accelerator acknowledges writes before they are fully committed to disk, speeding up writes and increasing optimization. The HP EFS WAN Accelerator does not acknowledge the file close until the file is safely written.

- **Enable CIFS Transparent Prepopulation**. To enable CIFS transparent prepopulation you must have the HP EFS Remote Copy Utility. The HP EFS Remote Copy Utility enables you to efficiently mirror data on the client and server. Because the data has already been copied to the client and server, the HP EFS WAN Accelerator only copies new data, increasing optimization of traffic across the WAN.

To enable CIFS options

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Protocols in the left menu to display the Setup: Protocols, CIFS page.

Figure 2-19. Setup: Protocols, CIFS page



3. Under General, click **Disable Write-Optimization** to disable write-through on CIFS traffic. Disabling CIFS write-optimization can decrease optimization on the HP EFS WAN Accelerator.
4. Under Transparent Prepopulation, click **Enable Transparent Prepopulation Support** to enable maximum optimization of data.
5. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)
6. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Setting MAPI Options

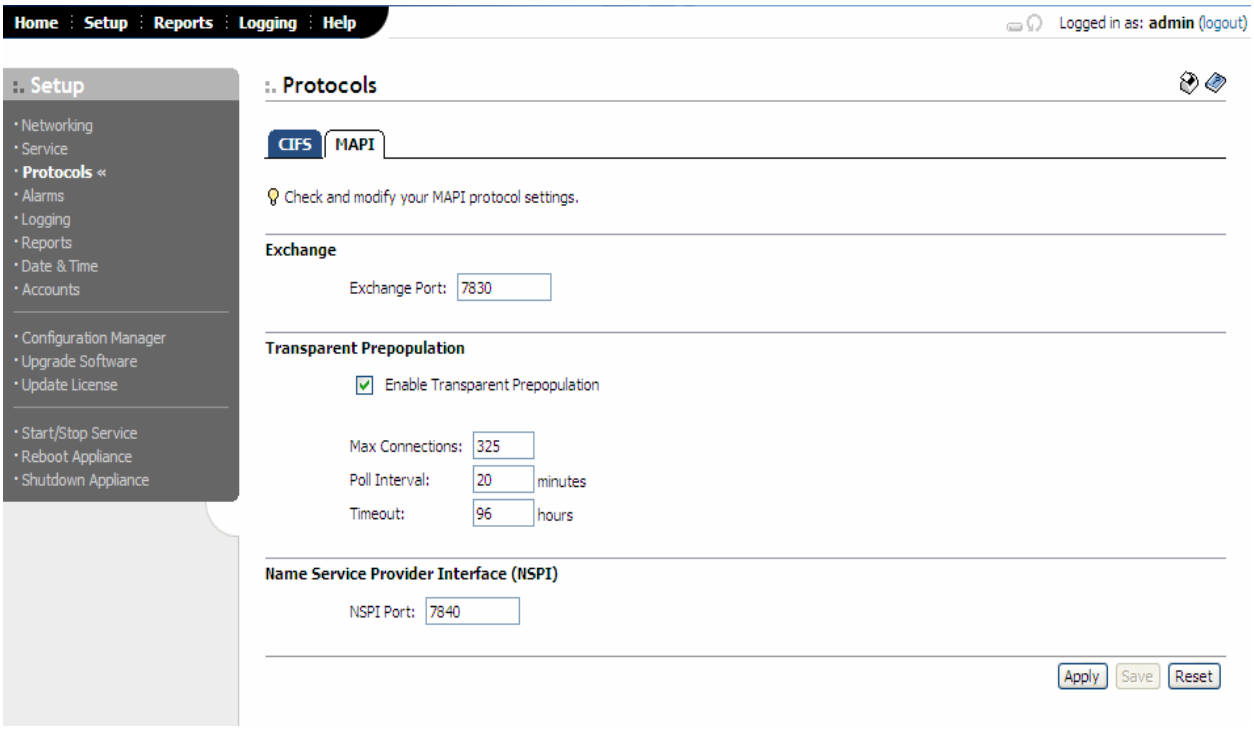
You configure the following features in the Setup: Protocols, MAPI page:

- **Exchange Port.** Configure the Exchange port if you have an internal firewall. This option is not commonly set.
- **MAPI Transparent Prepopulation**. MAPI transparent prepopulation allows mail data to be delivered between the Exchange server and the client-side HP EFS WAN Accelerator while the Outlook client is offline. When a user logs into their MAPI client, the mail is already waiting in the client-side HP EFS WAN Accelerator and can be retrieved locally. This feature enables mail to be optimized even though it has not been seen before by the client.
- **NSPI Port**. In certain situations (for example, clients connecting through a firewall), you might want to force a server to listen on a single pre-defined port so that access to ports can be controlled or locked down on the firewall.

To set MAPI options

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Protocols in the left menu to display the Setup: Protocols, CIFS page.
3. Click the MAPI tab to display the Setup: Protocols, MAPI page.

Figure 2-20. Setup: Protocols, MAPI page



4. Under Exchange, type a port number in the **Exchange Port** text box.
5. Under Transparent Prepopulation, click **Enable Transparent Prepopulation** to enable maximum optimization of mail data.
6. Type a number in the **Max Connections** text box to set the maximum number of virtual MAPI connections to the Exchange server for Outlook clients that have shut down. Setting the maximum connections limits the aggregate load on all Exchange servers through the configured HP EFS WAN Accelerator.

NOTE: You must configure the maximum connections on the client and server-side of the network.

---

7. Type the number of minutes in the **Poll Interval** text box to set the amount of time that you want the HP EFS WAN Accelerator to poll for shut down clients.

8. Type the time out number in seconds in the **Timeout** text box to suspend virtual MAPI connections. After the timeout has been exceeded, the virtual MAPI connection is terminated. The time out is enforced on a per-connection basis. The default value is **96** hours. Time out prevents a buildup of stale or unused virtual connections over time.

9. Under Name Service Provider Interface (NSPI), type a port number in the **NSPI Port** text box. Set this port to force a server to listen on a single pre-defined port so that access to ports is controlled or locked down on a firewall.

10. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)

11. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Setting Alarms and Fault Reporting

The following section describes how to set alarm thresholds, email notification parameters for events and failures, and Simple Network Management Protocol (SNMP) communities and traps. It contains the following sections:

Setting Alarm Thresholds

You set alarm thresholds, the stale data store, extended memory paging, and software mismatch alarms in the Setup: Alarms, Alarms page.

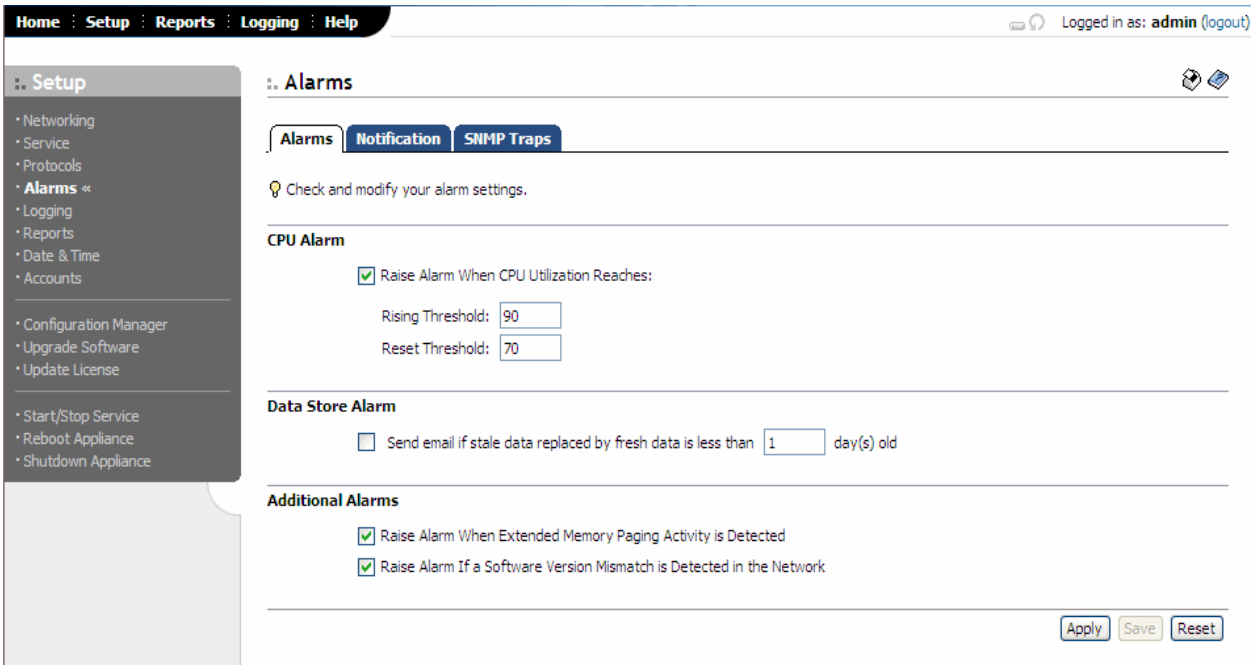
Alarms have rising and reset thresholds. When an alarm reaches the rising threshold, it is activated; it is reset when it reaches the lowest or reset threshold. After an alarm is triggered, it is not triggered again until it has fallen below the reset threshold.

To set the alarm threshold

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

2. Click Alarms in the left menu to display the Setup: Alarms, Alarms page.

Figure 2-21. Setup: Alarms, Alarms Page



3. Under CPU Alarm, click **Raise Alarm When CPU Utilization Reaches** and type a percentage in the **Rising Threshold** and **Reset Threshold** text boxes.

4. Under Data Store Alarm, click the check box and type a number in the **Send email if stale data replaces fresh data is less than ____ day(s) old** text box. You receive email notification when the data in the data store is replaced with new data before the time period specified.

5. Under Additional Alarms, click **Raise Alarm When Extended Memory Paging Activity Detected** to raise an alarm when abnormal memory page swapping occurs.

6. Click **Raise Alarm if A Software Version Mismatch Is Detected in the Network** to raise an alarm if the system detects that an HP EFS WAN Accelerator is running an incompatible version of the HP EFS WAN Accelerator software.

7. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)

8. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Setting Fault Notification

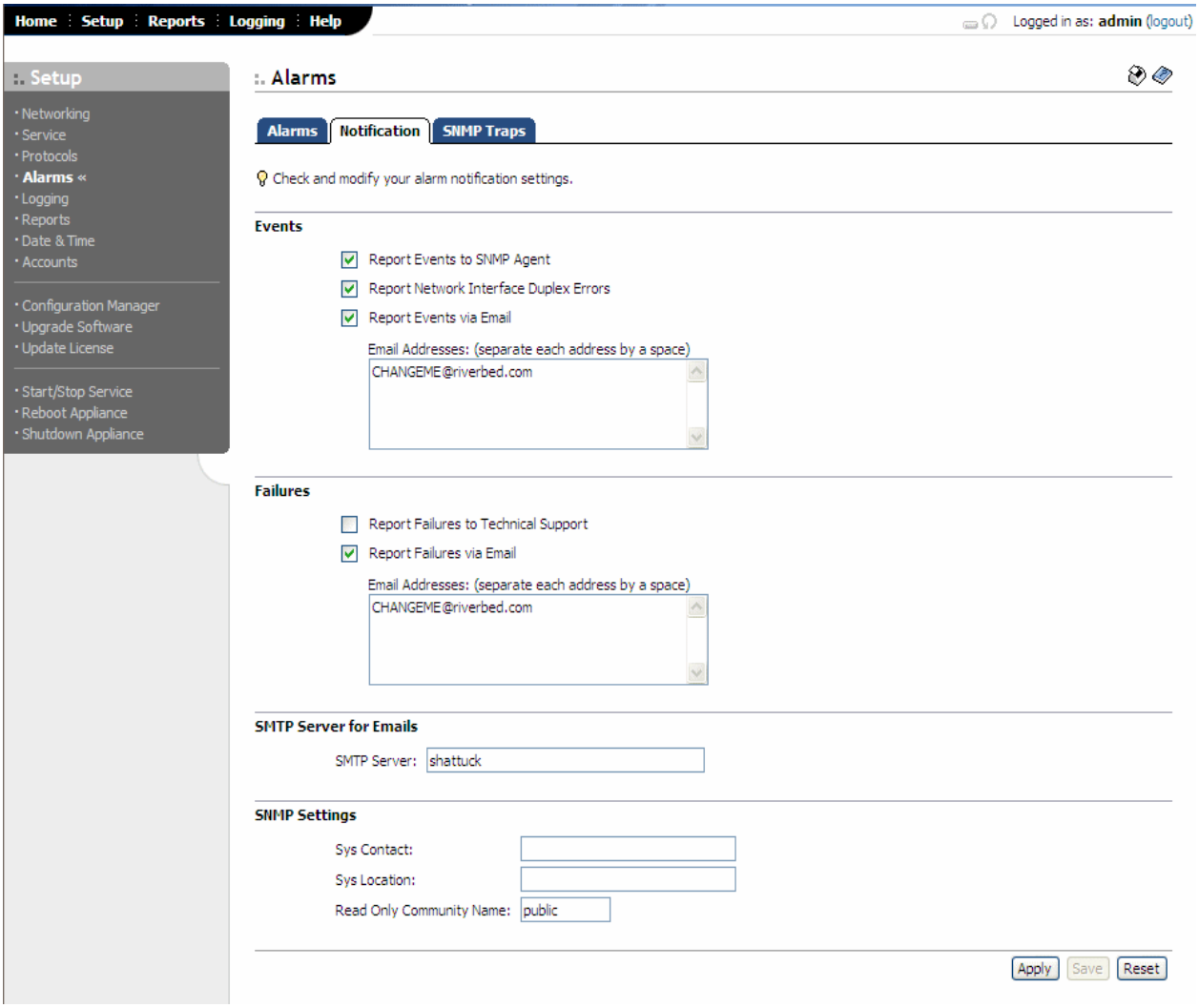
You set email notification parameters for events and failures in the Setup: Alarms, Notification page.

IMPORTANT: Make sure you provide a valid Simple Mail Transfer Protocol (SMTP) server to ensure that the users you specify receive email notifications for events and failures.

To set event and failure notification

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Alarms in the left menu to display the Setup: Alarms page.
3. Click the Notification tab to display the Setup: Alarms, Notification page.

Figure 2-22. Setup: Alarms, Notification Page



4. Under Events, click **Report Events to SNMP Agent** to report activity to an SNMP agent.

5. Click **Report Network Interface Duplex Errors** to report duplex errors and type the email addresses of the users you want to notify of duplex errors in the **Email Addresses** text box. Separate each email address by a space.

6. Click **Report Failures via Email** and type the email addresses of the users you want to notify of events in the **Email Addresses** text box. Separate each email address by a space.

7. Under Failures, click **Report Failures to Technical Support** to have serious failures such as system crashes reported to HP Technical Support. HP recommends that you activate this feature so that problems are promptly corrected.

8. Click **Report Failures via Email** and type the email addresses of the users you want to notify of failures in the **Email Addresses** text box. Separate each email address by a space.

9. Under SMTP Server for Emails, type a valid SMTP server in the **SMTP Server** text box.

NOTE: External DNS and external access for SMTP traffic is required for this feature to function.

---

10. Under SNMP Settings, type the SNMP contact in the **Sys Contact** text box.

11. Type the SNMP location in the **Sys Location** text box.

12. Type the read-only community name in the **Read Only Community Name** text box. This is the read-only string that gathers status and statistics from the edge border router. For example: **ReAdOnLy**.

13. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)

14. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

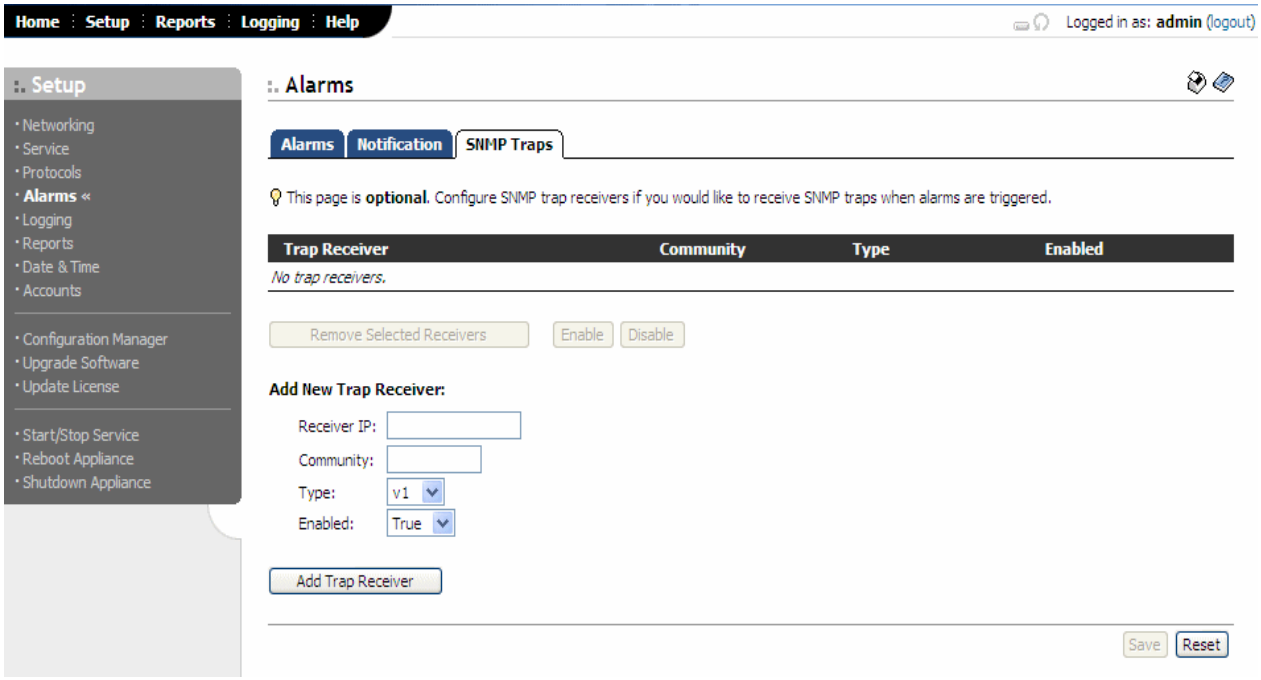
Setting SNMP Traps

Optionally, set SNMP traps in the Setup: Alarms, SNMP Traps page. Traps are messages sent by an SNMP agent that indicate the occurrence of an event.

To set an SNMP trap

1. Click the Setup tab to display the Setup: Networking, Names & Interfaces page.
2. Click Alarms in the left menu to display the Setup: Alarms page.
3. Click the SNMP Traps tab to display the Setup: Alarms, SNMP Traps page.

Figure 2-23. Setup: Alarms, SNMP Traps Page



4. Under Add New Trap Receiver, type the IP address for the SNMP trap in the **Receiver IP** text box.
5. Type the SNMP community name in the **Community** text box.
6. Select the SNMP version number either **v1** or **v2** from the **Type** drop-down list.
7. Select **True** or **False** from the **Enabled** drop-down list to enable or disable SNMP traps.
8. Click **Add Trap Receiver** to apply the settings to the running configuration.
9. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove an SNMP trap receiver, click the check box next to the name and click **Remove Selected Receivers**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To disable an SNMP trap receiver, click the check box next to the name and click **Disable**. To enable an SNMP trap receiver, click the check box next to the name and click **Enable**.

Setting Logging Options

The following section describes how to set local and remote logging for the HP EFS WAN Accelerator. It contains the following sections:

- "Setting Local Logging," next
- "Setting Remote Logging Servers" on page 69

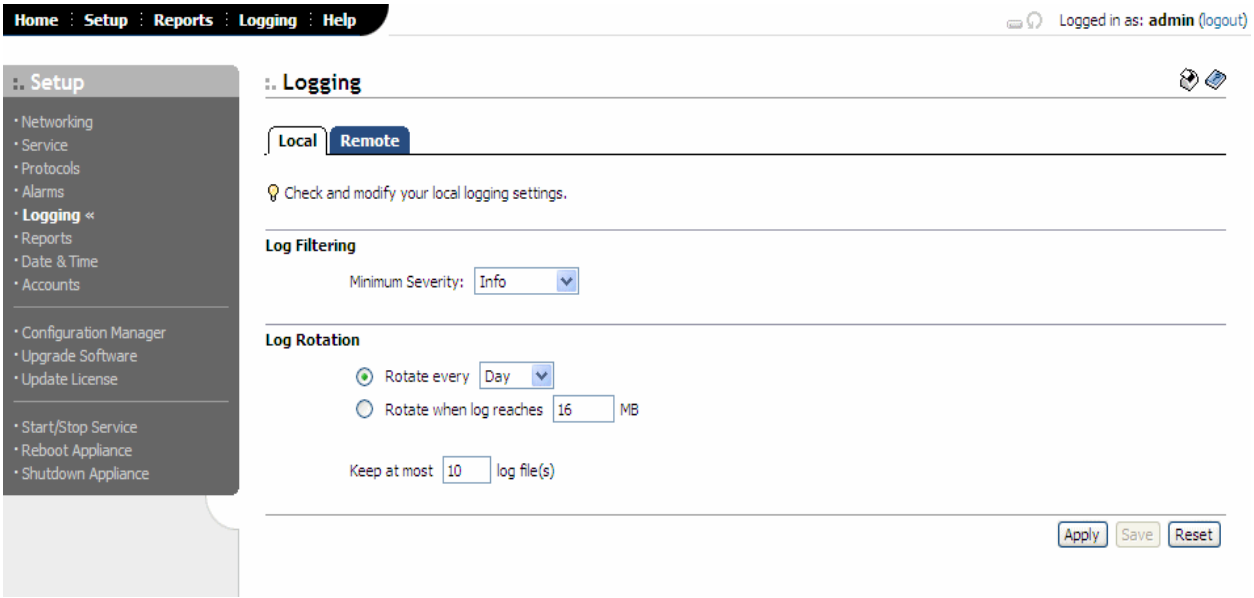
Setting Local Logging

You set log severity levels and rotation parameters for local logs in the Setup: Logging, Local page.

To set the log severity level and log rotation

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Logging in the left menu to display the Setup: Logging, Local page.

Figure 2-24. Setup: Logging, Local Page



3. Under Log Filtering, select a severity level from the **Minimum Severity** drop-down list.
4. Under Log Rotation, click **Rotate Every** and select **Day**, **Week**, or **Month** from the drop-down list to rotate logs according to a specific time period.
5. Click **Rotate when log reaches** and type a number to rotate logs according to a log file size.
6. Type a number in the **Keep at most** text box to set a limit for the number of logs to store.
7. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)
8. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

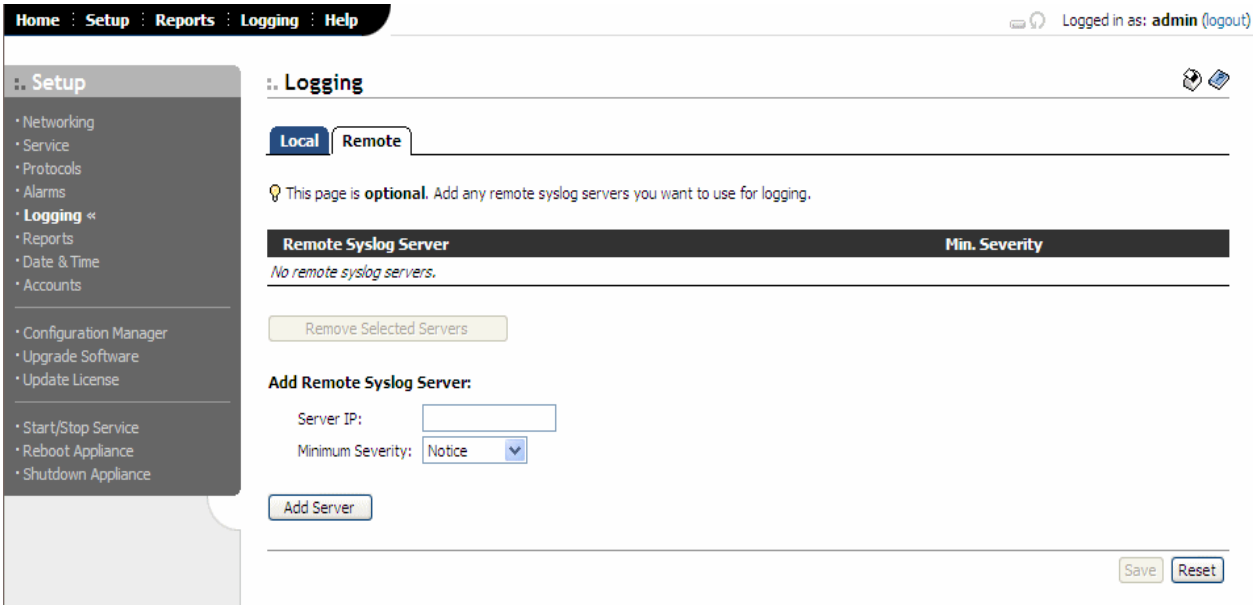
Setting Remote Logging Servers

Optionally, you set remote system log (**syslog**) servers in the Setup: Networking, Logging, Remote page.

To set a remote system log server

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Logging in the left menu to display the Setup: Logging page.
3. Click the Remote tab to display the Setup: Logging, Remote page.

Figure 2-25. Setup: Logging, Remote Page



4. Under Add Remote Syslog Server, type the IP address for the remote server in the **Server IP** text box.

5. Select the severity level for the logs from the **Minimum Severity** drop-down list.

6. Click **Add Server** to apply your settings to the running configuration.

7. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove a remote server, click the check box next to the name and click **Remove Selected Servers**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Setting Report Parameters

The following section describe how to set the ports to be monitored for performance reports.

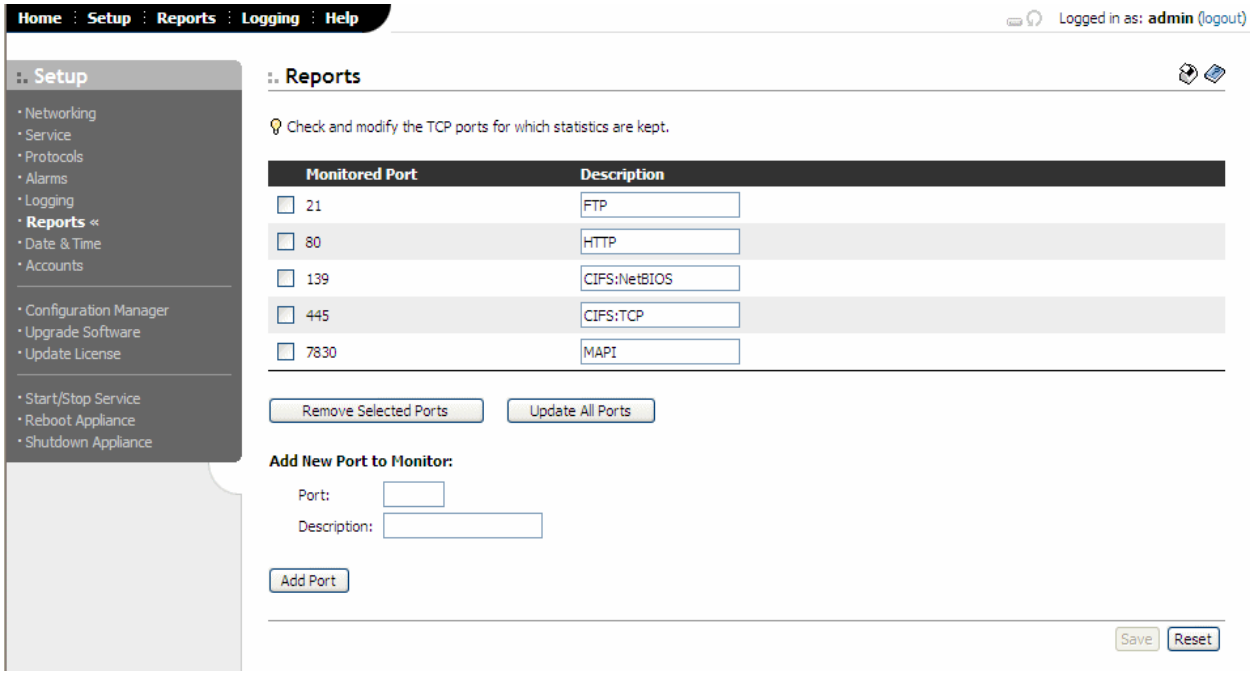
Setting Monitored Ports

You set the ports you want to monitor for performance reports in the Setup: Reports, Monitored Ports page.

To set a monitored port

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Reports in the left menu to display the Setup: Reports page.
3. Click the Monitored Ports tab to display the Setup: Reports page.

Figure 2-26. Setup: Reports Page



4. Under Add New Port to Monitor, type the port and a short description for the type of traffic in the **Port** and **Description** text boxes.
5. Click **Add Port** to apply your settings to the running configuration.
6. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove a port, click the check box next to the name and click **Remove Selected Ports**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To edit the description of a port, click **Update All Ports**.

Setting the Date and Time

The following section describes how to set the date and time or Network Time Protocol (NTP) servers for the HP EFS WAN Accelerator. It contains the following sections:

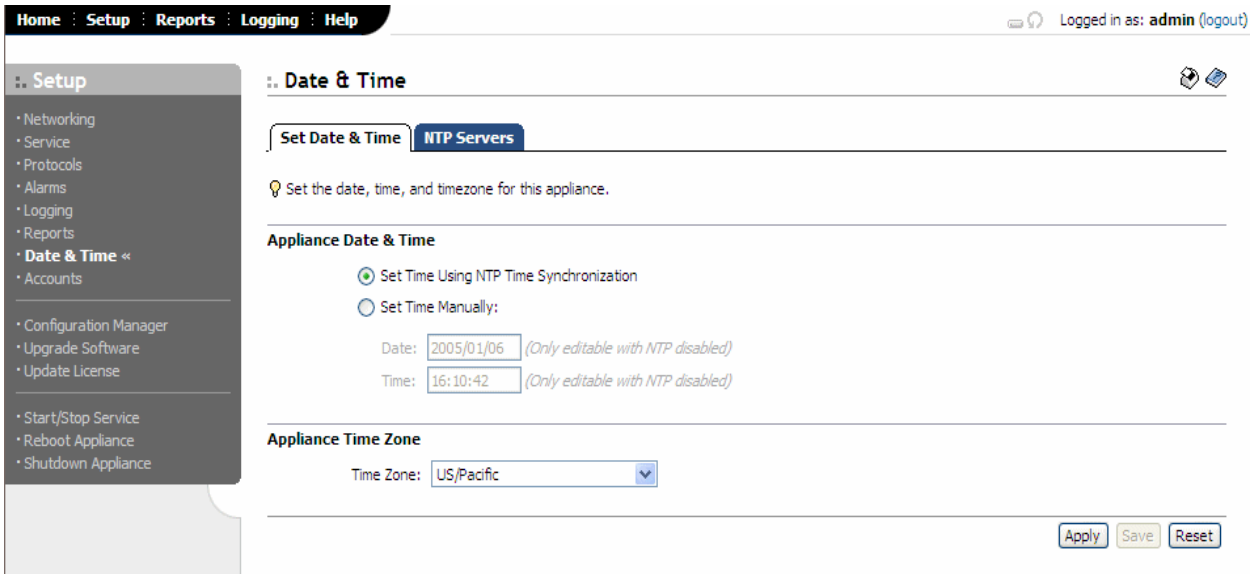
Setting the Date and Time

You set the date and time for the HP EFS WAN Accelerator in the Setup: Date & Time page.

To set the date and time

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Date & Time in the left menu to display the Setup: Date & Time, Set Date & Time page.

Figure 2-27. Setup: Date & Time, Set Date & Time Page



3. Under Appliance Date & Time, choose a method for determining the date and time:
   - Click **Set Time Using NTP Time Synchronization** if you want to synchronize the date and time using NTP synchronization. (Enabling NTP time synchronization enables the time stamps on the HP EFS WAN Accelerator logs to match those of other computers using NTP time synchronization. This option is not required for proper HP EFS WAN Accelerator operation.)
   - Click **Set Time Manually** if you want to manually set the date and time.
   - Type the current date in the **Date** text box. Use the following format: `YYYY/MM/DD`.

- Type the current time in the **Time** text box. Use the following format: `HH:MM:SS`.

4. Under Appliance Time Zone, select your time zone from the **Time Zone** drop-down list. The default time zone is **GMT** (Greenwich Mean Time).

NOTE: If you change the time zone, log messages from the kernel retain the old time zone until you reboot the HP EFS WAN Accelerator.

---

5. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)

6. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: If you change from NTP synchronization to manual synchronization, click **Set Time Manually** and click **Apply**. Type the date and time in the **Date** and **Time** text boxes and click **Apply** to apply your manual settings.

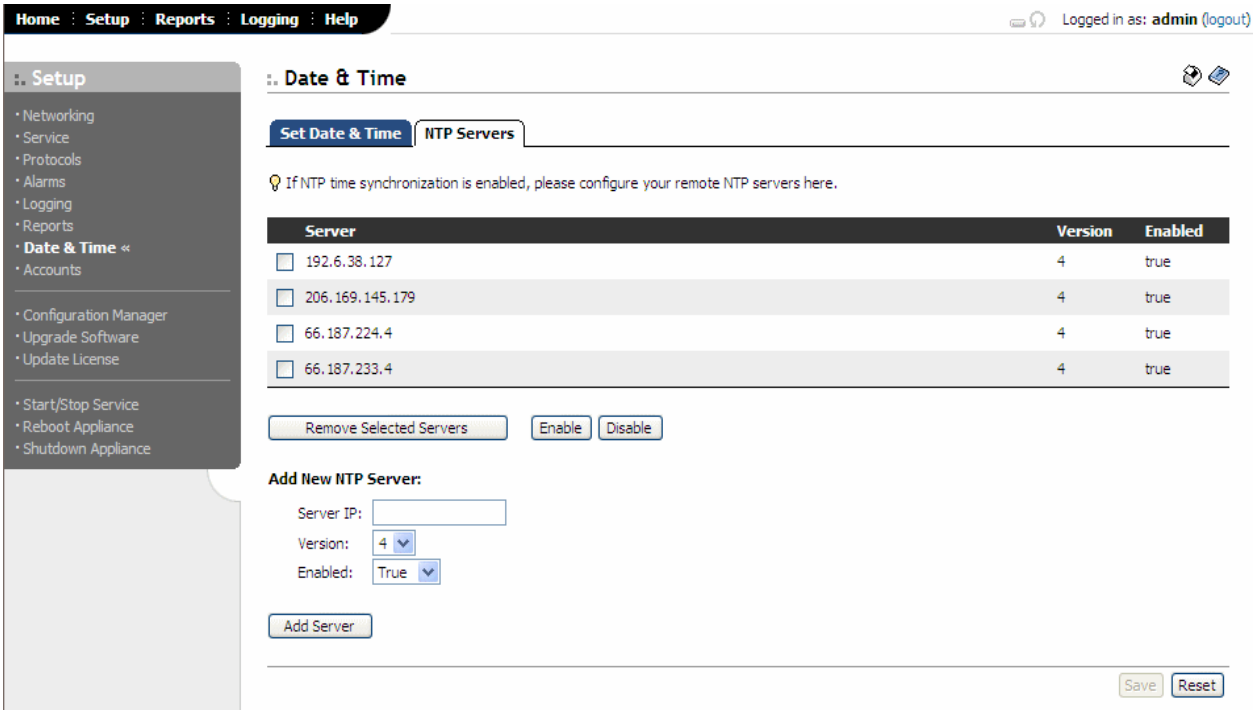
Setting NTP Servers

If you enabled NTP synchronization, set your NTP servers in the Setup: Date & Time, NTP Servers page. Enabling NTP time synchronization enables your logs to be synchronized. Time synchronization is not required for HP EFS WAN Accelerator operation.

To set an NTP server

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Date & Time in the left menu to display the Setup: Date & Time page.
3. Click the NTP Servers tab to display the Setup: Date & Time, NTP Servers page.

Figure 2-28. Setup: Date & Time, NTP Servers Page



4. Under Add New NTP Server, type the IP address for the NTP server in the **Server IP** text box.
5. Select the NTP protocol version number from the **Version** drop-down list.
6. Select the mode, either **True** or **False** from the **Enable** drop-down list. The **True** value enables synchronization. The **False** value disables synchronization.
7. Click **Add Server** to apply the settings to the running configuration.
8. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove an NTP server, click the check box next to the name and click **Remove Selected Servers**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To disable synchronization for a server, click the check box next to the NTP server name and click **Disable**. To enable synchronization for a server, click the check box next to the NTP server name and click **Enable**.

Managing Accounts

The following section describes how to set administrator and monitor passwords, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System (TACACS+) authentication. It contains the following sections:

Setting Authentication Methods

You can prioritize local, RADIUS, and TACACS+ authentication methods for the system and set the authorization policy and default user for RADIUS and TACACS+ authorization systems in the Setup: Accounts, General page.

IMPORTANT: Make sure to put the authentication methods in the order in which you want authentication to occur. If authorization fails on the first method, the next method is attempted, and so forth, until all the methods have been attempted.

TIP: To set TACACS authorization levels (**admin** or **read-only**) to allow certain members of a group to log in, add the following attribute to **users** on the TACACS server:

```
service = rbt-exec {
      local-user-name = "monitor"
 }
```

where you replace **monitor** with **admin** for write access.

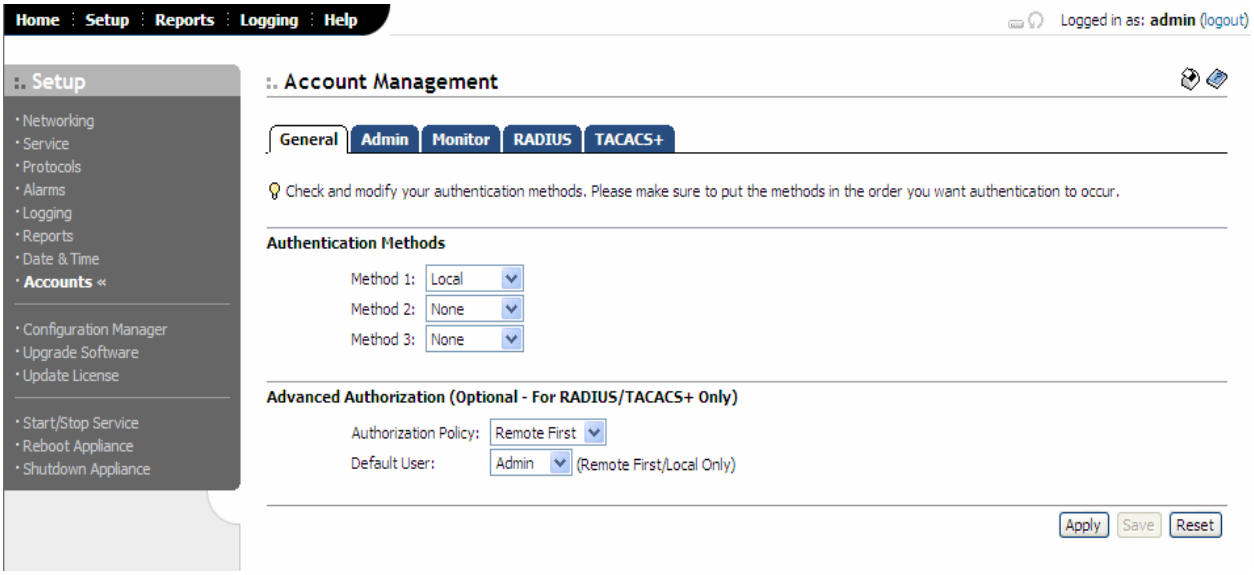
For detailed information about configuring RADIUS and TACACS+ servers to accept login requests from the HP EFS WAN Accelerator, see the *HP EFS WAN Accelerator Command Line Interface Reference Manual*.

To set an authentication method

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

2. Click Accounts in the left menu to display the Setup: Account Management, General page.

Figure 2-29. Setup: Account Management, General Page



3. Under Authentication Methods, select **Local**, **RADIUS**, or **TACACS+** from the **Method 1** drop-down list. Make sure you put the authentication methods in the order in which you want them to occur.

If authorization fails on the first method, the next method is attempted, and so forth, until all the methods have been attempted.

4. Select **None**, **Local**, **RADIUS**, or **TACACS+** from the **Method 2** drop-down list.
5. Select **None**, **Local**, **RADIUS**, or **TACACS+** from the **Method 3** drop-down list.
6. Optionally, under Advanced Authentication, select **Remote First**, **Remote Local**, or **Remote Only** from the **Authentication Policy** drop-down list.
7. Optionally, under Advanced Authentication, select **Admin** or **Monitor** from the **Default User** drop-down list.
8. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before committing it memory.)
9. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Setting the Administrative Password

During the initial setup of the HP EFS WAN Accelerator you set the administrator password. Check or modify your setting in the Setup: Account Management page. (The default administrator password is **password**.)

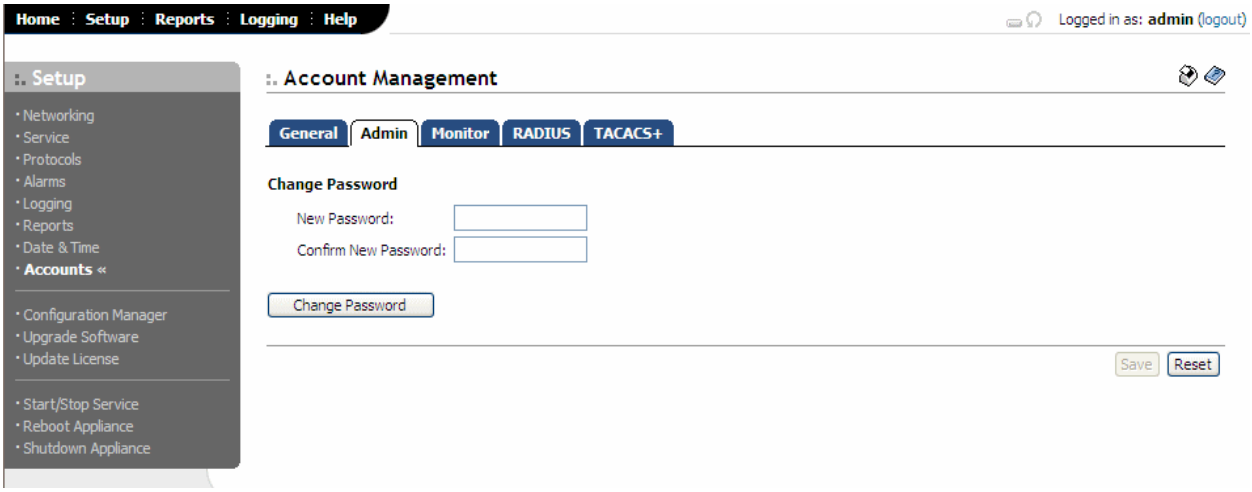
The administrator user has full privileges in the HP EFS WAN Accelerator. For example, as an administrator you can set and modify configuration settings, restart the HP EFS WAN Accelerator service, reboot the appliance, and create and view performance and system reports.

The password must have a minimum of 6 characters.

To set the administrator password

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Accounts in the left menu to display the Setup: Account Management, Admin page.

Figure 2-30. Setup: Account Management, Admin Page



3. Under Change Password, type the new administrative password in the **New Password** text box. The password must have a minimum of 6 characters.

4. Retype the new administrative password in the **Confirm New Password** text box.

5. Click **Change Password** to apply your settings to the running configuration.

6. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

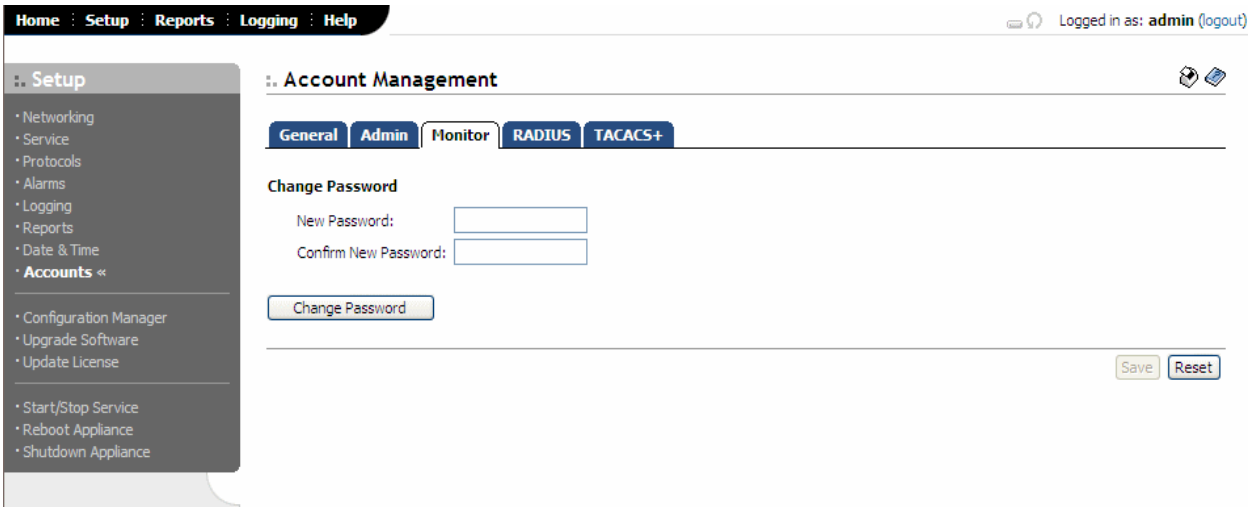
Setting the Monitor Password

You set the monitor user password in the Setup: Account Management page. A monitor user can view connected HP EFS WAN Accelerators and reports; a monitor user cannot make configuration changes to the HP EFS WAN Accelerator. The password must have a minimum of 6 characters.

To set the monitor password

1. Click the Setup tab to display the Setup: Networking Name & Interfaces page.
2. Click Accounts in the left menu to display the Setup: Account Management, Admin page.
3. Click the Monitor tab to display the Setup: Account Management, Monitor page.

Figure 2-31. Setup: Account Management, Monitor Page.



4. Under Change Password, type the new monitor password in the **New Password** text box. The password must have a minimum of 6 characters.
5. Retype the new monitor password in the **Confirm New Password** text box.
6. Click **Change Password** to apply your settings to the running configuration.
7. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

Configuring RADIUS Server Authentication

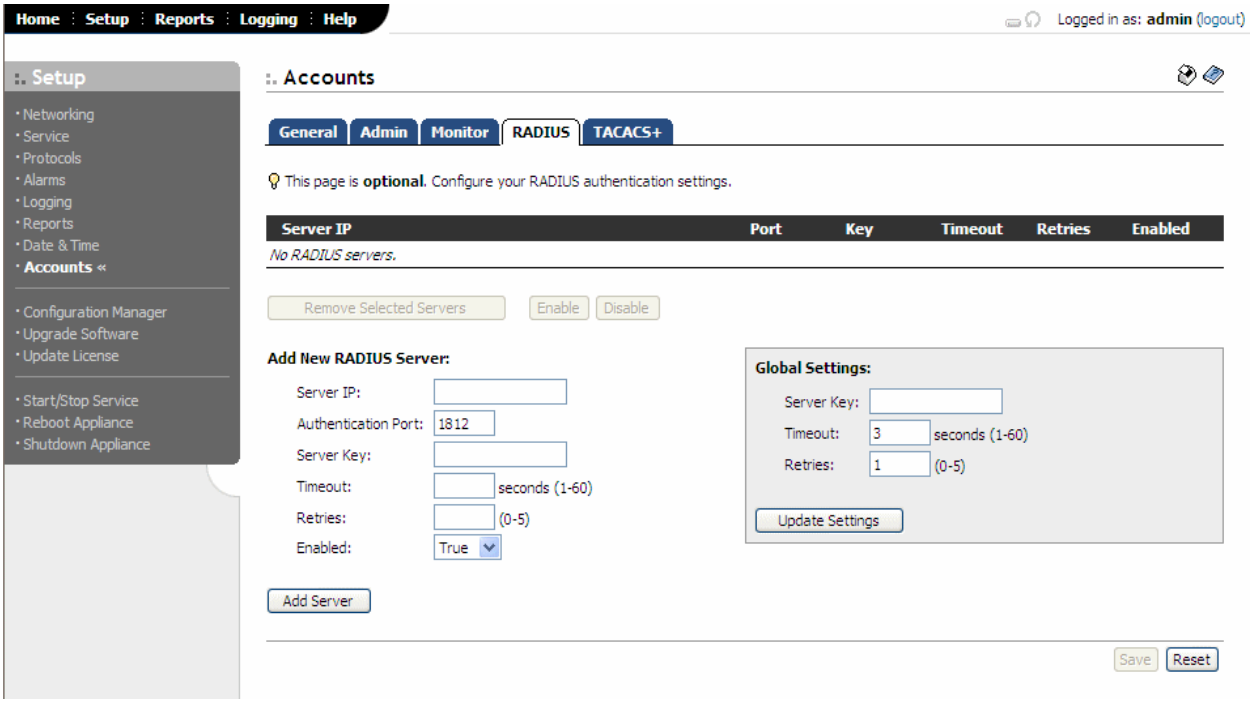
Optionally, configure RADIUS authentication in the Setup: Accounts, RADIUS page. RADIUS is an access control protocol that uses a challenge and response method for authenticating users.

For detailed information about configuring RADIUS and TACACS+ servers to accept login requests from the HP EFS WAN Accelerator, see the *HP EFS WAN Accelerator Command Line Interface Reference Manual*.

To configure RADIUS server authentication

1. Click the Setup tab to display the Setup: Networking Name & Interfaces page.
2. Click Accounts in the left menu to display the Setup: Account Management, Admin page.
3. Click the RADIUS tab to display the Setup: Account Management, RADIUS page.

Figure 2-32. Setup: Account Management, RADIUS Page.



4. Under Add New RADIUS Server, type the RADIUS server IP address in the **Server IP** text box.
5. Type the port for the RADIUS server in the **Authentication Port** text box.
6. Type the server key in the **Server Key** text box.
7. Type the timeout period in the **Timeout** text box.
8. Select **True** or **False** from the **Enabled** drop-down list to enable or disable the server.
9. Click **Add Server** to apply your settings to the running configuration.
10. Under Global Settings, type the server key in the **Server Key** text box.
11. Type the timeout period in the **Timeout** text box.
12. Type the number of time you want to allow the user to retry authentication in the **Retries** text box.
13. Click **Update Settings** to update your global RADIUS settings.
14. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove a server, click the check box next to the name and click **Remove Selected Servers**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To disable authentication for a server, click the check box next to the server name and click **Disable**. To enable authentication for a server, click the check box next to the server name and click **Enable**.

Configuring TACACS+ Server Authentication

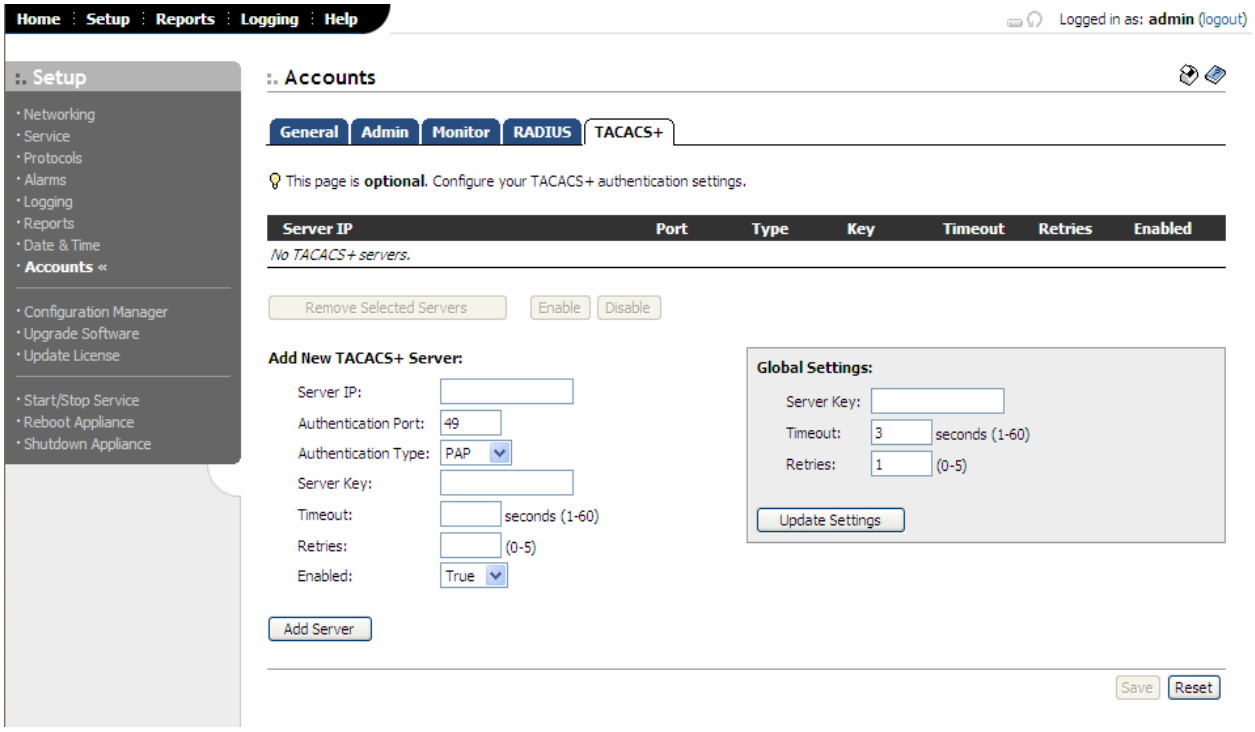
Optionally, configure TACACS+ server authentication in the TACACS+ in the Setup: Accounts, TACACS+ page. TACACS+ is an authentication protocol that allows a remote access server to forward a login password for a user to an authentication server to determine whether access is allowed to a given system.

For detailed information about configuring RADIUS and TACACS+ servers to accept login requests from the HP EFS WAN Accelerator, see the *HP EFS WAN Accelerator Command Line Interface Reference Manual*.

To configure a TACACS+ server

1. Click the Setup tab to display the Setup: Networking Name & Interfaces page.
2. Click Accounts in the left menu to display the Setup: Account Management, Admin page.
3. Click the TACACS+ tab to display the Setup: Account Management, TACACS+ page.

Figure 2-33. Setup: Account Management, TACACS+ Page.



4. Under Add New TACACS+ Server, type the TACACS+ server IP address in the **Server IP** text box.
5. Type the port for the TACACS+ server in the **Authentication Port** text box.
6. Type the server key in the **Server Key** text box.
7. Type the timeout period in the **Timeout** text box.
8. Select **True** or **False** from the **Enabled** drop-down list to enable or disable the server.
9. Click **Add Server** to apply your settings to the running configuration.
10. Under Global Settings, type the server key in the **Server Key** text box.
11. Type the timeout period in the **Timeout** text box.
12. Type the number of time you want to allow the user to retry authentication in the **Retries** text box.
13. Click **Update Settings** to update your global TACACS+ settings.
14. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To remove a server, click the check box next to the name and click **Remove Selected Servers**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

TIP: To disable authentication for a server, click the check box next to the server name and click **Disable**. To enable authentication for a server, click the check box next to the server name and click **Enable**.

Managing Configurations

The following section describes how to save, import, and activate a configuration for the HP EFS WAN Accelerator. After you have finished the configuration process you must write your settings to memory.

Writing Configurations to Memory

Each HP EFS WAN Accelerator has an active, running configuration and written, saved configurations. You can save your settings on each individual page of the Management Console or you can apply your settings to make sure that the values you set are correct before you save the configuration.

When you **Apply** your settings in the Management Console the values are applied to the current running configuration—it does not write the settings to memory. When you **Save** your configuration settings, the values are written to memory and take effect after you restart the HP EFS WAN Accelerator service.

Each time you save your configuration settings, they are written to the current running configuration, and a backup is created. For example, if the running configuration is **myconfig** and you save it, **myconfig** is backed up to **myconfig.bak** and **myconfig** is overwritten with the current configuration settings.

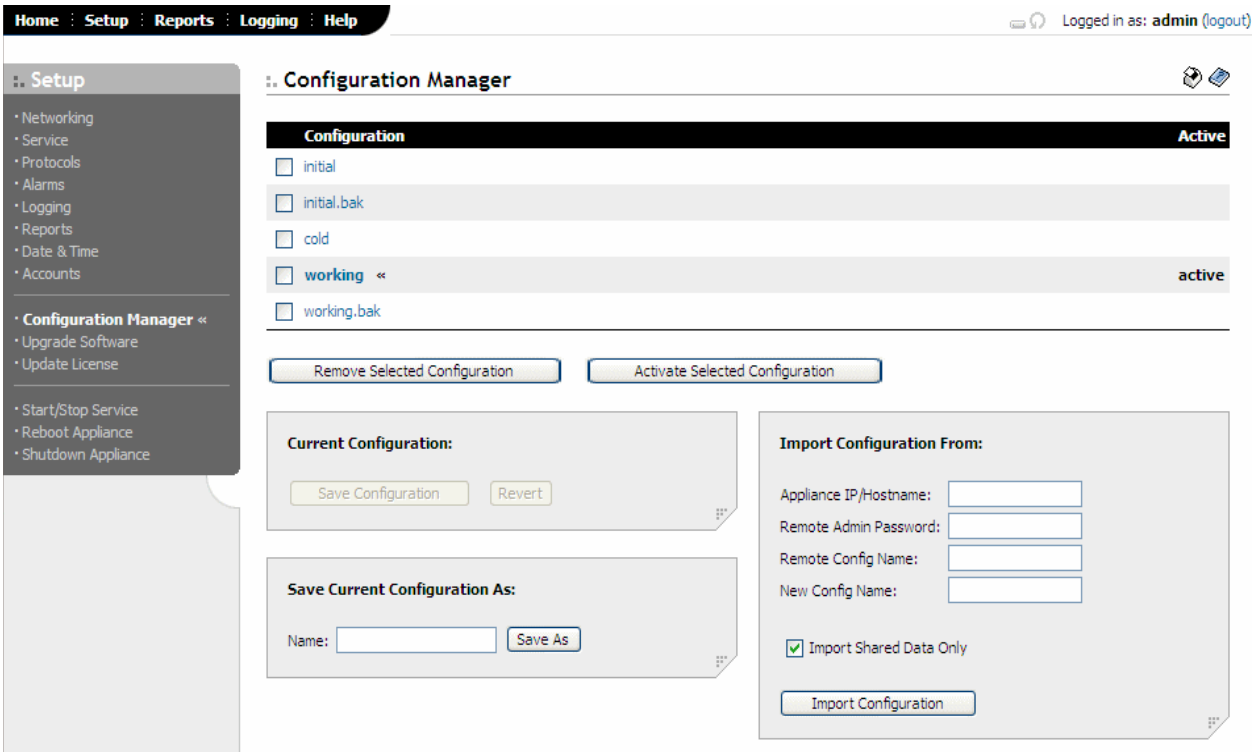
TIP: If you have not saved your settings, the **Save Configuration** icon turns orange in the left side of the page.

IMPORTANT: Some configuration settings require you to restart the HP EFS WAN Accelerator service for the settings to take effect. For detailed information about restarting the HP EFS WAN Accelerator service, see "Starting, Stopping, and Restarting the HP EFS WAN Accelerator Service" on page 94.

To write configuration settings to memory

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Configuration Manager in the left menu to display the Setup: Configuration Manager page.

Figure 2-34. Setup: Configuration Manager Page



3. Click **Save Configuration** to write the configuration to memory or **Revert** to revert to the running configuration.

TIP: To save the configuration with a new name, under **Save Current Configuration As** type a name in the Name text box and click **Save As**.

TIP: To remove a configuration, click the check box next to the name and click **Remove Selected Configuration**. Click **Save Configuration** to write your settings to memory or click **Revert** to return your settings to their previous values.

IMPORTANT: You must restart the HP EFS WAN Accelerator service for a configuration to take effect. For detailed information, see "Starting, Stopping, and Restarting the HP EFS WAN Accelerator Service" on page 94.

Importing Configurations

You can import a configuration from one HP EFS WAN Accelerator to another.

You can avoid copy and paste errors by using the import configuration option when you are replacing or adding an HP EFS WAN Accelerator in your network. Simply connect the replacement HP EFS WAN Accelerator to your LAN and import the configuration from your existing HP EFS WAN Accelerator. If you are swapping one HP EFS WAN Accelerator for another, you can import all of the network information (although not the licenses) and disconnect the old HP EFS WAN Accelerator before you switch configurations on the new appliance.

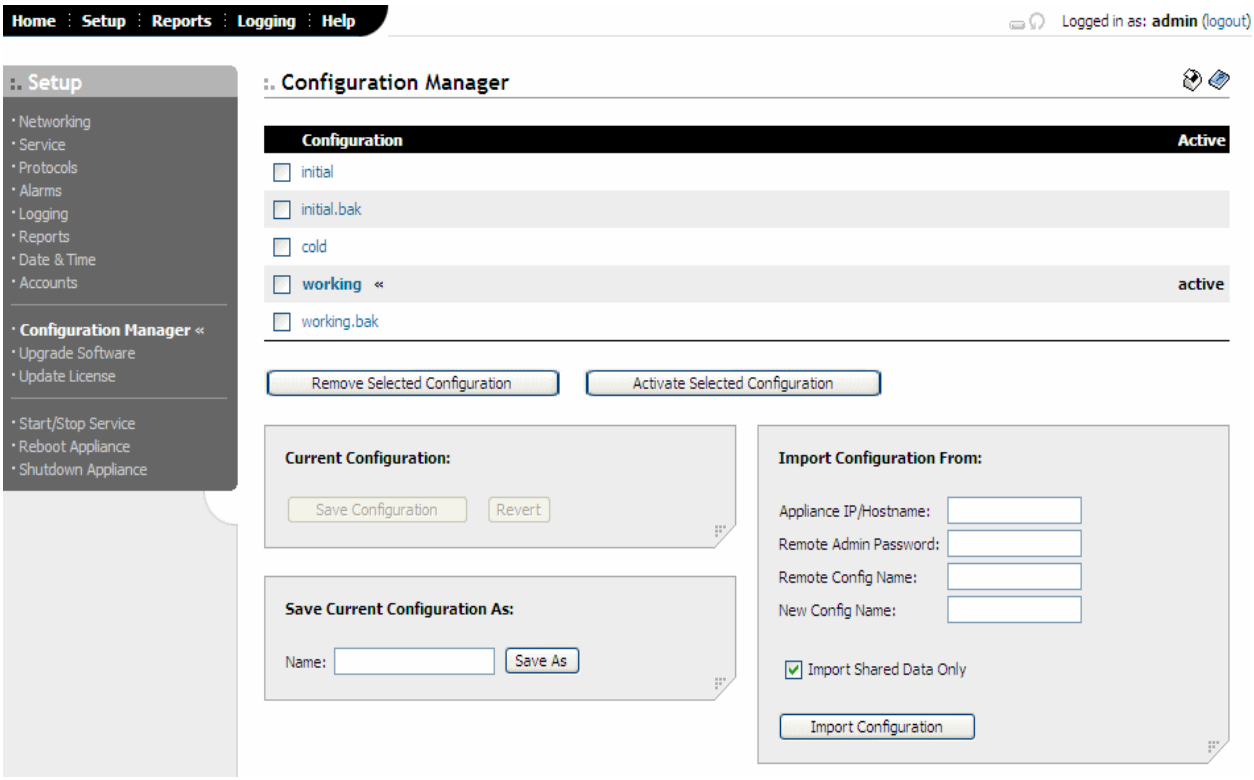
To deploy a large network of HP EFS WAN Accelerators, you can avoid configuring each appliance individually by setting up a template appliance and using the configuration import option to copy the template to each appliance.

To import a configuration

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

2. Click Configuration Manager in the left menu to display the Setup: Configuration Manager page.

Figure 2-35. Setup: Configuration Manager Page



3. Under Import Configuration From, type the IP address or host name of the HP EFS WAN Accelerator from which you want to import the configuration in the **Appliance IP/Hostname** text box.

4. Type the password for the remote HP EFS WAN Accelerator in the **Remote Admin Password** text box.

5. Type the name of the configuration you want to import from the remote HP EFS WAN Accelerator in the **Remote Config Name** text box.

6. Type a new, local, configuration name for this HP EFS WAN Accelerator in the **New Config Name** text box.

7. Optionally, uncheck **Import Shared Data Only** to import all of the configuration settings for the remote HP EFS WAN Accelerator.

WARNING: This action copies unique settings such as network settings.

Keep **Import Shared Data Only** checked to copy only the following common settings:

- in-path and out-of-path interface
- protocols
- CLI and Web
- statistics, NTP, SNMP, and alarm

The following settings are not automatically copied:

- failover
- SNMP (contact and location) and log
- network settings

8. Click **Import Configuration** to import the configuration settings to the HP EFS WAN Accelerator.

   The imported configuration appears in the Configuration list.

Activating Configurations

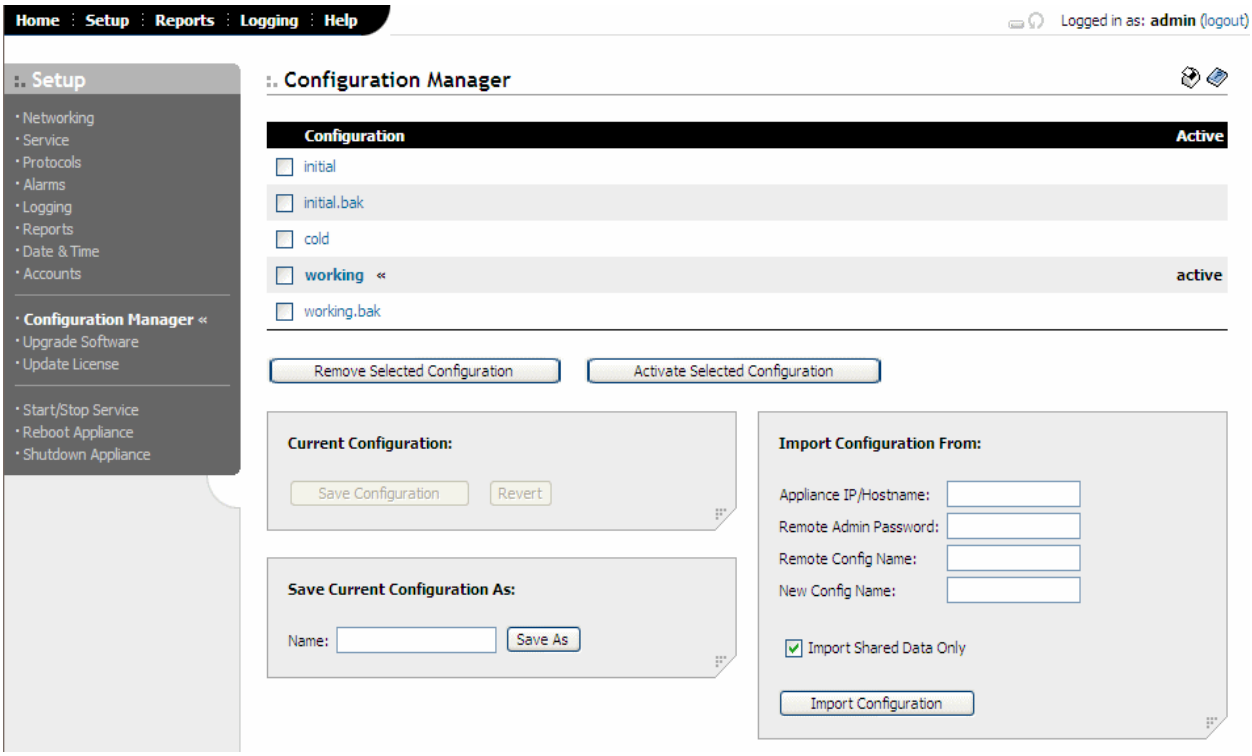
You can activate a previous configuration. When you activate a configuration it becomes the current, running configuration. To save your configuration settings, see "To write configuration settings to memory" on page 84.

To activate a configuration

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

2. Click Configuration Manager in the left menu to display the Setup: Configuration Manager page.

Figure 2-36. Setup: Configuration Manager Page



3. In the Configuration list, click the check box next to the configuration you want to activate.

4. Click **Activate Selected Configuration** to activate the configuration. When you activate a configuration, the settings in that configuration file become the running configuration.

5. Click **Save Configuration** to write the new configuration to memory or click **Revert** to revert to the running configuration.

IMPORTANT: You must restart the HP EFS WAN Accelerator service for this configuration to take effect. For detailed information, see "Starting, Stopping, and Restarting the HP EFS WAN Accelerator Service" on page 94.

TIP: To delete configurations, in the Configuration list, click the check box next to the name of the configuration you want to delete and click **Remove Selected Configuration**.

TIP: To revert to the running configuration, click **Revert**.

Upgrading Your Software

The following section describes how to upgrade to a new version of the HP EFS WAN Accelerator software and how to revert to a previous version of the HP EFS WAN Accelerator software.

Upgrading Your Software

You can upgrade the HP EFS WAN Accelerator software from a Uniform Resource Locator (URL) or from a local file in the Setup: Software Upgrade page. You can also revert to a previous version of the software.

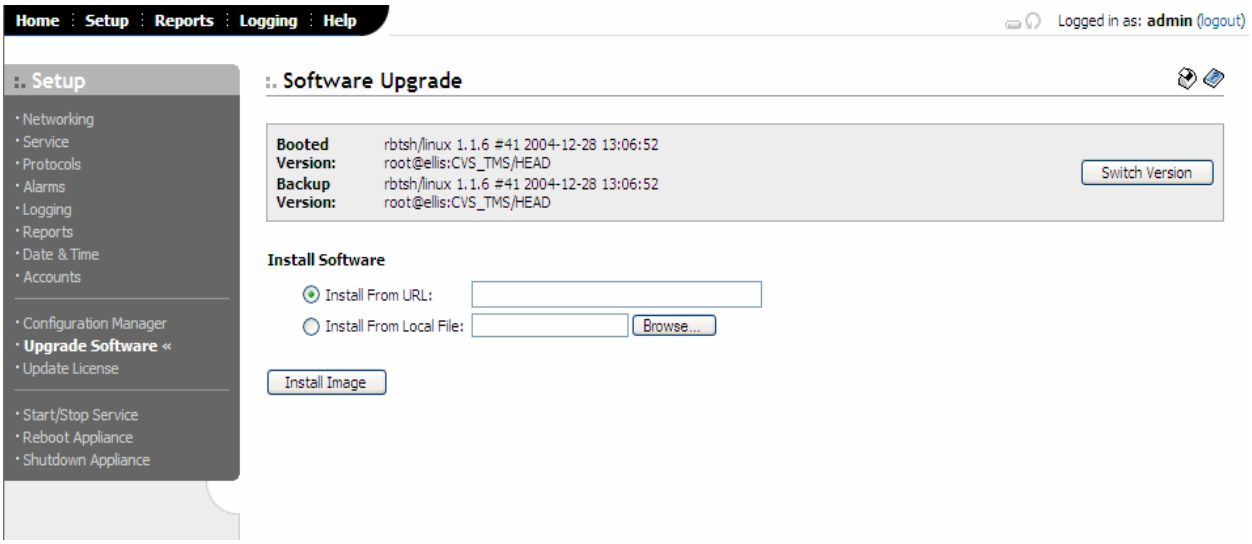
NOTE: HTTP (Hyper Text Transfer Protocol) and File Transfer Protocol (FTP) URLs are valid.

To upgrade your software

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.

2. Click Upgrade Software in the left menu to display the Setup: Software Upgrade page.

Figure 2-37. Setup: Software Upgrade Page



3. Under Install Software, choose a method for installing the new software:

   - Click **Install from a URL** and type the URL in the text box to install the software from a URL.
   - Click **Install From Local File** and type the path to install from a file on a Web browser machine. (To browse to the local file directory, click **Browse**.)

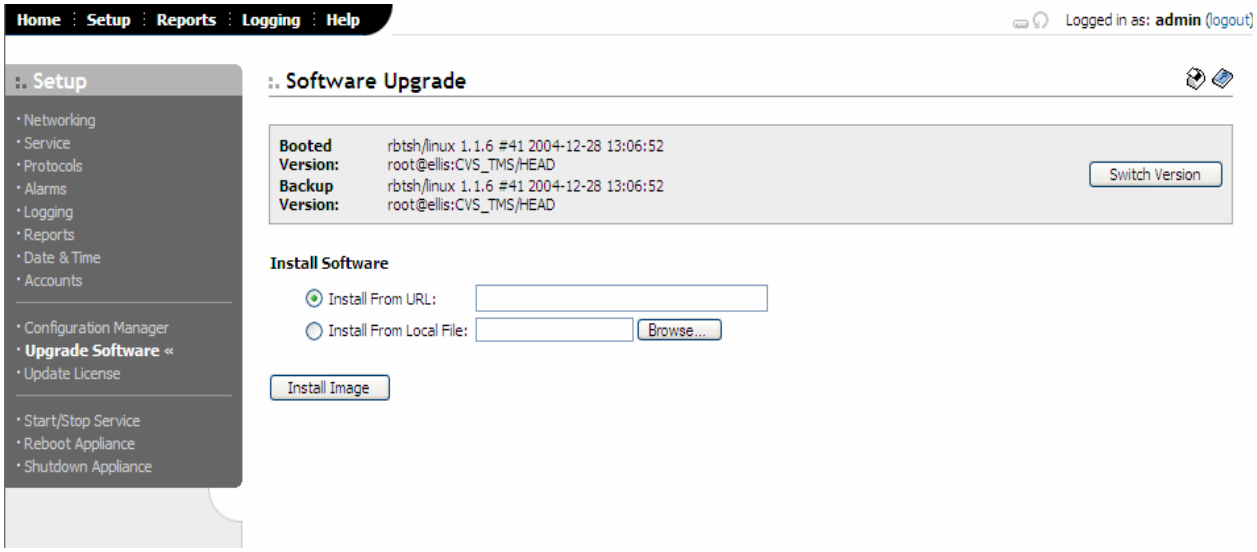
4. Click **Install Image** to install the new version of the software.

You can revert to a previous version of the software. The previous version of the software is displayed in the Setup: Software Upgrade page.

To revert to a previous version of the software

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Upgrade Software in the left menu to display the Setup: Software Upgrade page.

Figure 2-38. Setup: Software Upgrade Page



3. In the Software Upgrade section, click **Switch Version** next to the software version that you want to install. The previous version of the software is installed.

Updating Your License

The following section describes how to view current protocol accelerators and how to update your software license for the HP EFS WAN Accelerator. It contains the following sections:

- "Viewing Protocol Accelerators," next
- "Updating Your Licenses" on page 92

Viewing Protocol Accelerators

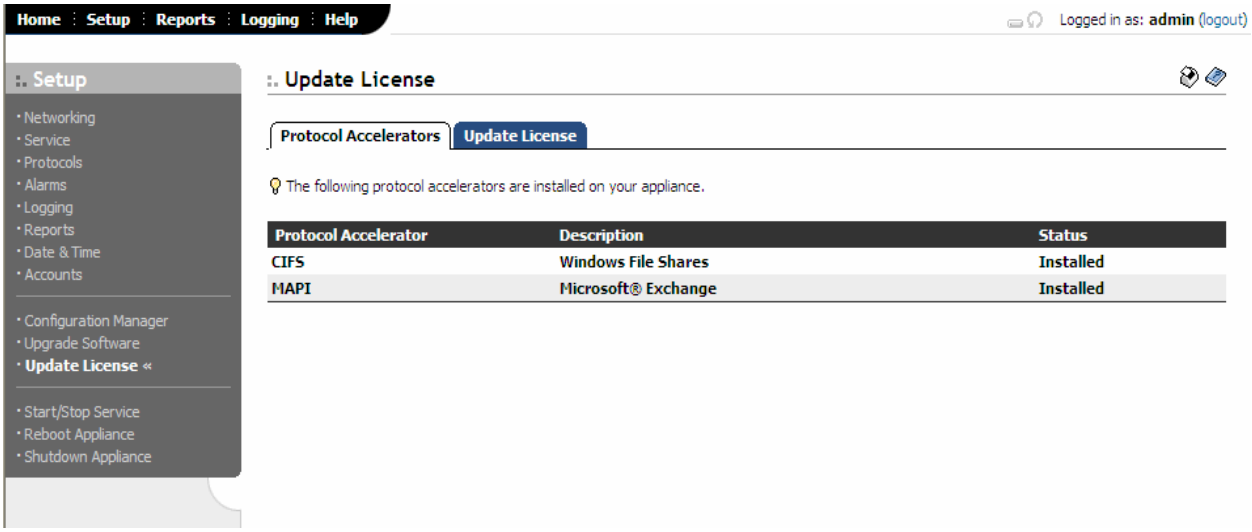
You can view the Protocol Accelerators installed on your system in the Setup: Update License, Protocol Accelerator page. A Protocol Accelerator is a blade installed on your system that optimizes a particular type of traffic such as CIFS or Exchange.

To view protocol accelerators

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Update License in the left menu to display the Setup: Update License, Protocol Accelerators page.

   The installed protocol accelerators, a description, and the status of the accelerator are listed in the Protocol Accelerator list.

Figure 2-39. Setup: Update License, Protocol Accelerators Page



Updating Your Licenses

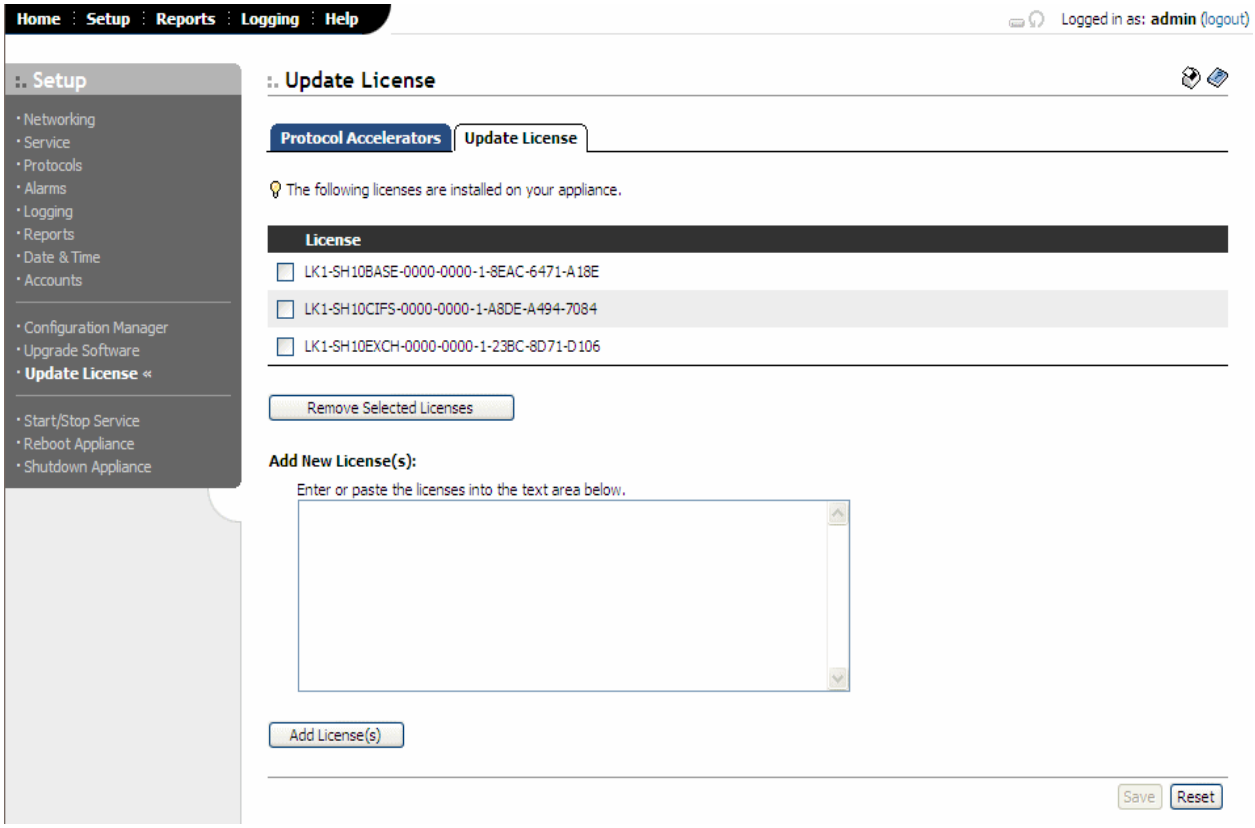
You can view a list of active licenses, update expired licenses, and add new license keys in the Setup: Update License, Update License page.

If you enter multiple license keys they must be separated by space, tab, or RETURN.

To update a license

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Update License in the left menu to display the Setup: Update License page.
3. Click the Update License tab to display the Setup: Update License, Update License page.

Figure 2-40. Setup: Update License, Update License Page



4. Copy and paste the license key in the **Add New License(s)** text box.
5. Click **Add License(s)** to add the license key to the running configuration.
6. Click **Save** to write the new license to memory or click **Reset** to return the settings to their previous values.

TIP: To remove a license, click the check box next to the name and click **Remove Selected Licenses**. Click **Save** to write your settings to memory or click **Reset** to return your settings to their previous values.

Starting, Stopping, and Restarting the HP EFS WAN Accelerator Service

The following section describes how to start, stop, and restart the HP EFS WAN Accelerator service.

Starting, Stopping, and Restarting the HP EFS WAN Accelerator Service

You can start, stop, and restart the HP EFS WAN Accelerator service in the Setup: Start/Stop Service page.

The HP EFS WAN Accelerator service is a daemon that executes in the background performing operations when required. Because many of the HP EFS WAN Accelerator service commands are initiated at startup, it is important to restart the HP EFS WAN Accelerator service when you have made changes to your configuration.

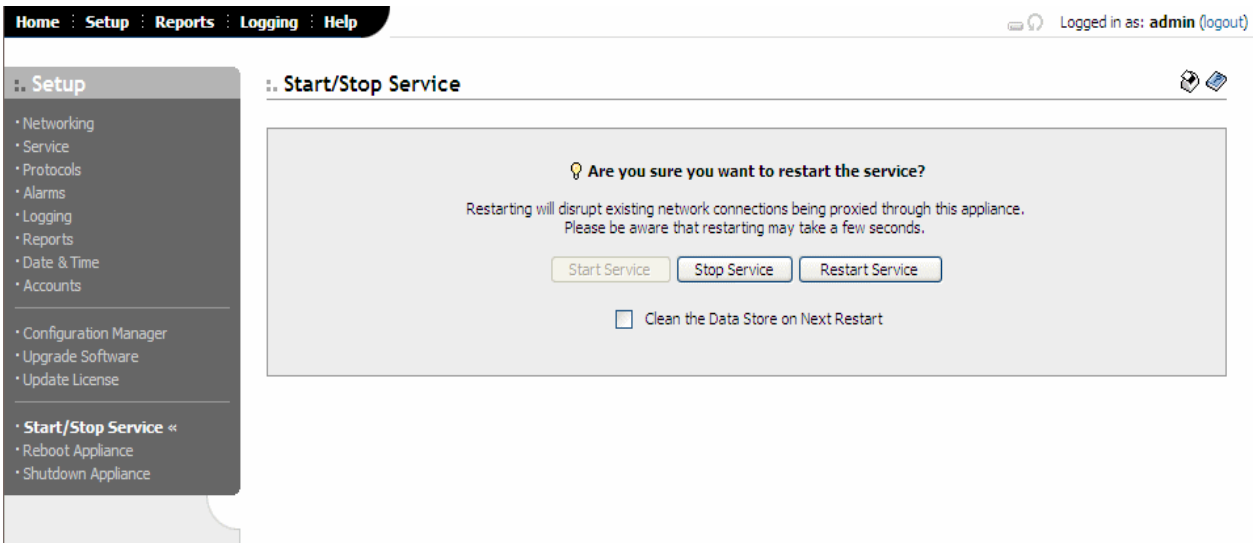
TIP: If you need to restart the HP EFS WAN Accelerator service, the **Restart Service** icon turns orange in the left side of the page

WARNING: Restarting the HP EFS WAN Accelerator service disrupts existing network connections that are proxied through the HP EFS WAN Accelerator.

To start the HP EFS WAN Accelerator service

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Start/Stop Service in the left menu to display the Setup: Start/Stop Service page.

Figure 2-41. Setup: Start/Stop Service Page



3. Click **Start Service** to start the HP EFS WAN Accelerator service. Starting the service takes a few seconds.

TIP: To stop the HP EFS WAN Accelerator service, click **Stop Service**. To restart the HP EFS WAN Accelerator service, click **Restart Service**.

TIP: To remove data from the data store, click **Clean the Data Store on Next Restart**. (You rarely need to clean the data store outside of the lab environment.)

Rebooting the HP EFS WAN Accelerator

The following section describes how to reboot the HP EFS WAN Accelerator.

Rebooting the HP EFS WAN Accelerator

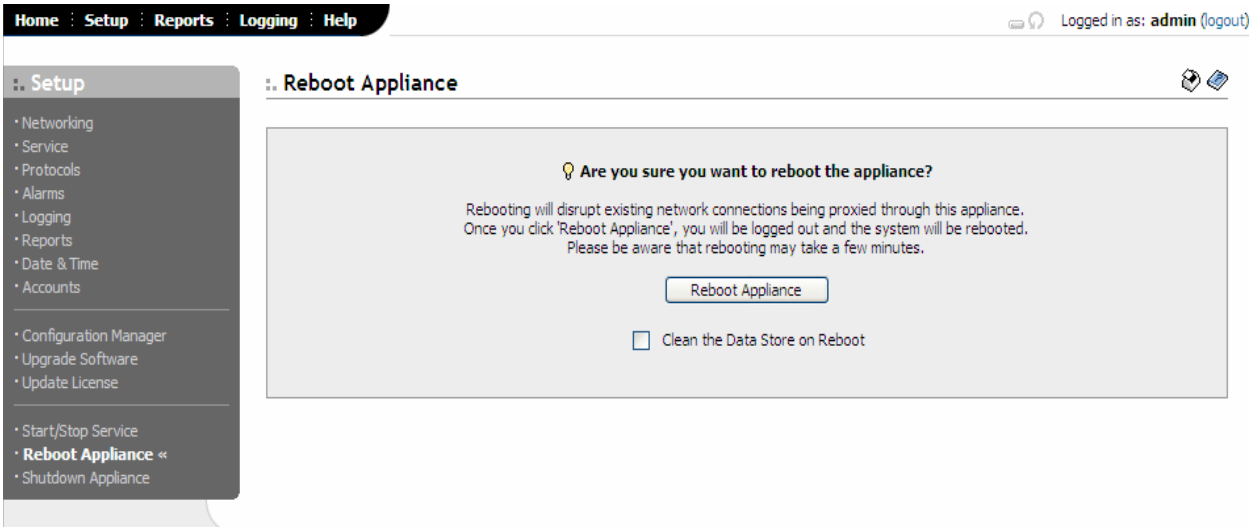
You reboot the HP EFS WAN Accelerator in the Setup: Reboot Appliance page.

Rebooting the HP EFS WAN Accelerator disrupts existing network connections that are currently proxied through the appliance. Rebooting can take a few minutes.

To reboot the HP EFS WAN Accelerator

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Reboot Appliance to display the Setup: Reboot Appliance page.

Figure 2-42. Setup: Reboot Appliance Page



3. Click **Reboot Appliance**. After you click **Reboot Appliance**, you are logged out of the system and it is rebooted.

Shutting Down the HP EFS WAN Accelerator

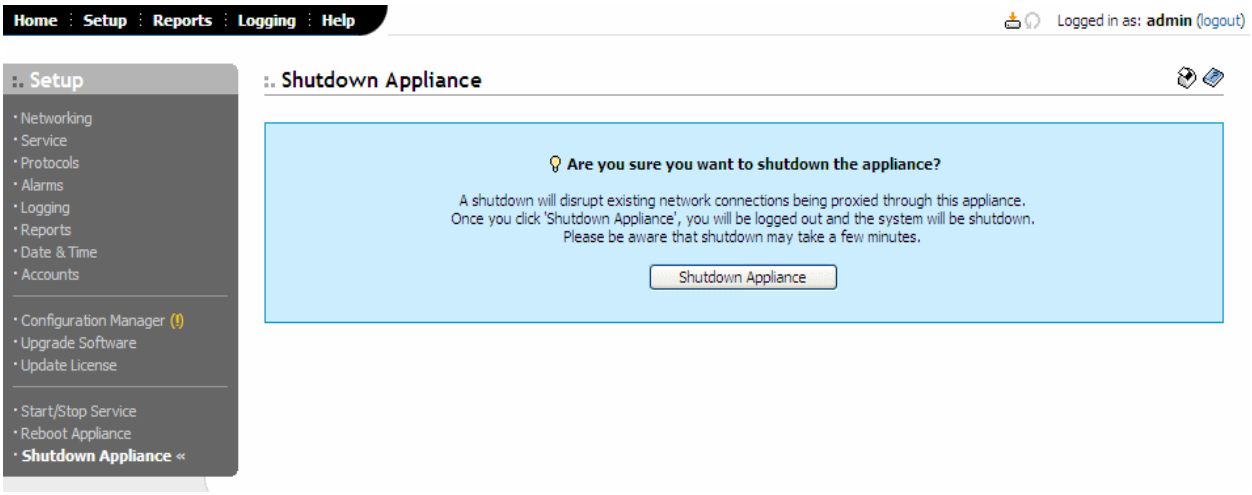
You shutdown the HP EFS WAN Accelerator in the Setup: Shutdown Appliance page. When you shutdown the HP EFS WAN Accelerator, connections are broken and optimization ceases. Shutdown can take a few minutes.

To restart the system you must manually turn on the HP EFS WAN Accelerator.

To shutdown the HP EFS WAN Accelerator

1. Click the Setup tab to display the Setup: Networking, Name & Interfaces page.
2. Click Shutdown Appliance to display the Setup: Shutdown Appliance page.

Figure 2-43. Setup: Shutdown Appliance Page



3. Click **Shutdown Appliance**. After you click **Shutdown Appliance**, the system is turned off. To restart the system you must manually turn on the HP EFS WAN Accelerator.

TIP: To remove data from the data store, click the **Clean the Data Store on Reboot** check box.

Creating HP EFS WAN Accelerator Reports

The Management Console provides performance, network, and HP EFS WAN Accelerator reports. The HP EFS WAN Accelerator provides performance and system reports as described in the following sections:

- "Creating Bandwidth Optimization Reports," next
- "Creating Traffic Summary Reports" on page 99
- "Creating Data Reduction by Application Reports" on page 100
- "Viewing the Network Diagram" on page 103

Creating Bandwidth Optimization Reports

The Performance: Bandwidth Optimization report summarizes the overall inbound and outbound bandwidth improvements for your network using the HP EFS WAN Accelerator. You can create reports according to the time period of your choice, application, and type of traffic.

The Bandwidth Optimization report includes the following table of statistics that describe bandwidth activity for the time period you specify.

Field	Description
WAN Data	Specifies the bandwidth utilized over the WAN using the HP EFS WAN Accelerator.
LAN Data	Specifies the bandwidth utilized over the LAN using the HP EFS WAN Accelerator.
Data Reduction %	Specifies the percent decrease of data transmitted over the WAN.
Peak Data Reduction %	Specifies the peak decrease in data transmitted over the WAN.
Capacity Increase	Specifies the increase in the amount of carrying capacity over the WAN.

What this Report Tells You

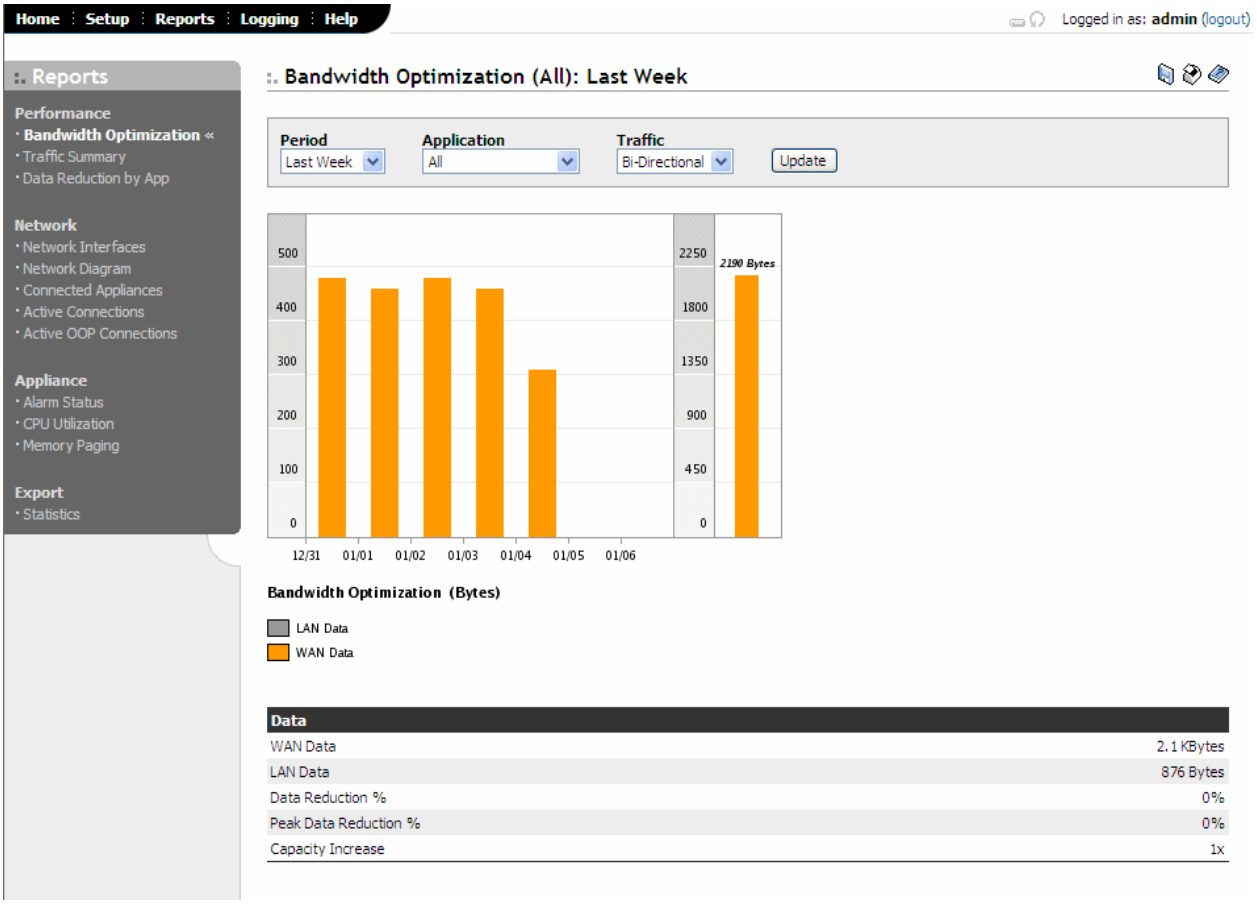
The Bandwidth Optimization report answers the following questions:

- How much bandwidth have I saved using the HP EFS WAN Accelerator?
- What was the average and peak amount of data sent?
- What was the rate at which data was sent?
- What was the overall increase in bandwidth capacity using the HP EFS WAN Accelerator?

To create a Bandwidth Optimization report

1. Click the Reports tab to display the Reports: Performance Summary page.
2. Click Bandwidth Optimization in the left menu to display the Reports: Bandwidth Optimization page.

Figure 2-44. Reports: Bandwidth Optimization Report



3. Select **Last Hour**, **Last Day**, **Last Week**, or **Last Month** from the **Period** drop-down list.
4. Select an application from the **Application** drop-down list. The default value is **All**.
5. Select **Bidirectional**, **LAN to WAN**, or **WAN to LAN** from the **Traffic** drop-down list.
6. Click **Update** to update your report.

TIP: To print your report, click the **Printer** icon in the upper right corner of the page.

TIP: Click the **Disk** icon in the upper right corner of the page to download your report statistics to your local disk in comma separated value (CSV) format. For detailed information about exporting statistics, see "Exporting Performance Statistics" on page 113.

Creating Traffic Summary Reports

The Reports: Traffic Summary report provides a percentage breakdown of the amount of traffic going through the system by application. You set the ports to be monitored in the Setup: Reports, Monitored Ports page.

NOTE: The Traffic Summary report displays a maximum of 16 colors for ports. If you have more than 16 ports, the colors in the report wrap from the beginning.

The Traffic Summary report contains the following table of statistics that summarize traffic activity by application.

Field	Description
Total Traffic	Specifies the total amount of traffic transmitted.
Total Passed Through (Unoptimized)	Specifies the amount of traffic transmitted unoptimized.
FTP	Specifies the amount of File Transfer Protocol (FTP) data transmitted.
HTTP	Specifies the amount of HyperText Transfer Protocol (HTTP) data transmitted.
CIFS: NetBIOS	Specifies the amount of data transmitted with NETBIOS over the Common Internet File System (CIFS) protocol.
CIFS: TCP	Specifies the amount of data transmitted with the CIFS protocol over Transmission Control Protocol (TCP).
MAPI	Specifies the amount of data transmitted over Messaging API (MAPI).
Other	Specifies the amount of data transmitted over other applications.

To monitor traffic other than the default traffic listed above, see "Setting Monitored Ports" on page 71.

What This Report Tells You

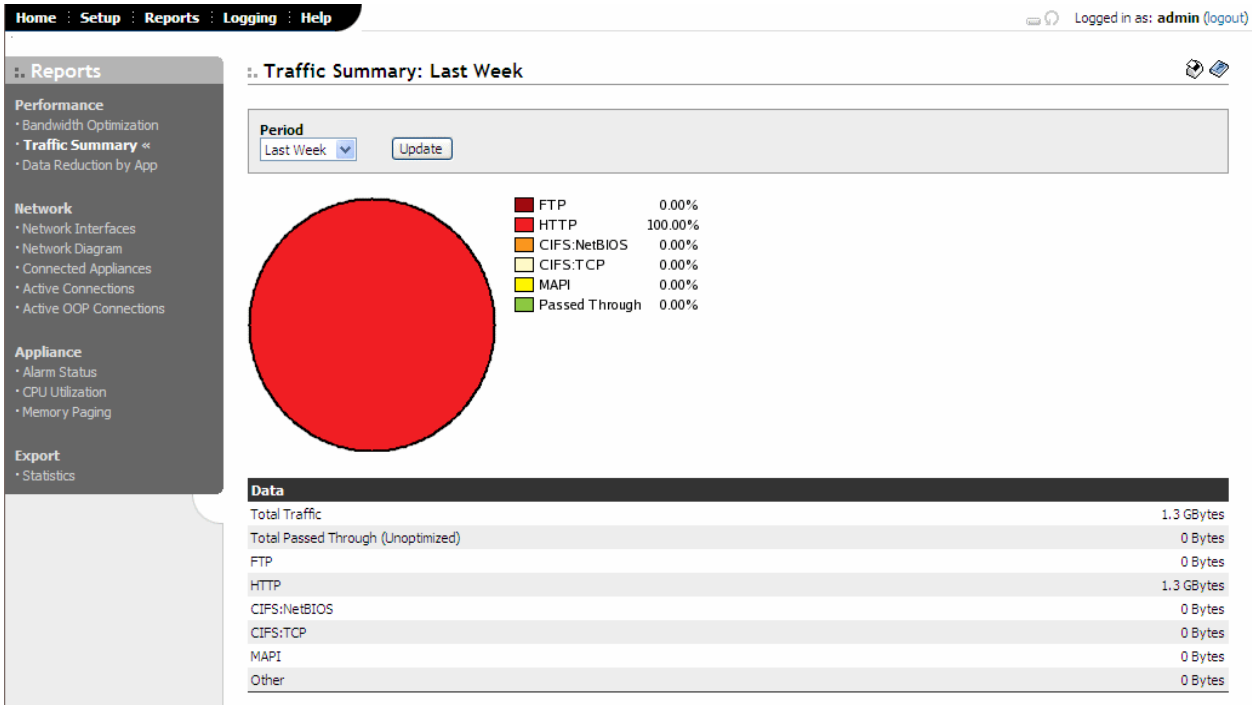
The Traffic Summary report answers the following questions:

- How much data was transmitted?
- How much data was transmitted unoptimized?
- How much data was transmitted over FTP, HTTP, CIFS, CIFS: NetBIOS, CIFS: TCP, and MAPI?

To create the Traffic Summary report

1. Click the Reports tab to display the Reports: Performance Summary page.
2. Click Traffic Summary in the left menu to display the Reports: Traffic Summary page.

Figure 2-45. Reports: Traffic Summary Report



3. Select **Last Hour**, **Last Day**, **Last Week,** or **Last Month** from the **Period** drop-down list.
4. Click **Update** to update your report.

TIP: To print your report, click the **Printer** icon in the upper right corner of the page.

Creating Data Reduction by Application Reports

The Reports: Data Reduction by Application report summarizes the percent reduction of data transmitted by application such as FTP, HTTP, NetBIOS and TCP traffic in CIFS, and Mail API (MAPI).

What This Report Tells You

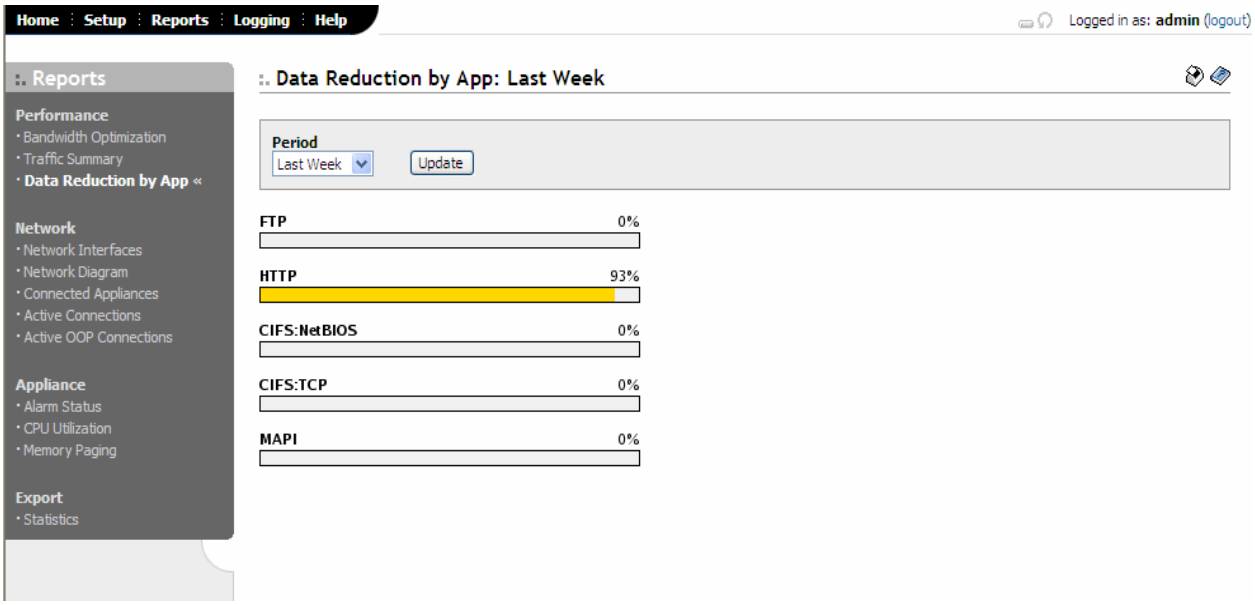
The Data Reduction by Application answers the following question:

- What was the percent reduction in the amount of data transmitted for each application?

To create the Data Reduction by Application report

1. Click the Reports tab to display the Reports: Performance Summary page.
2. Click Data Reduction by App in the left menu to display the Reports: Data Reduction by App page.

Figure 2-46. Reports: Data Reduction by Application Report



3. Select **Last Hour**, **Last Day**, **Last Week**, or **Last Month** from the **Period** drop-down list.
4. Click **Update** to update your report.

TIP: To print your report, click the **Printer** icon in the upper right corner of the page.

Viewing Network Interface Statistics

The Reports: Network Interfaces Statistics report summarizes the statistics for the primary, in-path LAN and WAN, and auxiliary interfaces. It also displays the IP address, speed, duplex, MAC address, and current status for each interface.

The Reports: Network Interfaces Statistics report displays the following statistics.

	Packet Type	Description
Primary Interface	RX Packets (Received)	Specifies the number of packets discarded, errors encountered, packets overrun, and **mcast** packets sent.
	TX Packets (Transmitted)	Specifies the number of packets discarded, errors encountered, packets overrun, carriers used, and collisions encountered.
In-Path LAN Interface	RX Packets (Received)	Specifies the number of packets discarded, errors encountered, packets overrun, frames sent, and **mcast** packets sent.
	TX Packets (Transmitted)	Specifies the number of packets discarded, errors encountered, packets overrun, carriers used, and collisions encountered.
In-Path WAN Interface	RX Packets (Received)	Specifies the number of packets discarded, errors encountered, packets overrun, frames sent, and **mcast** packets sent.
	TX Packets (Transmitted)	Specifies the number packets discarded, errors encountered, packets overrun, carriers used, and collisions encountered.
Auxiliary Interface	RX Packets (Received)	Specifies the number of packets discarded, errors encountered, packets overrun, and **mcast** packets sent.
	TX Packets (Transmitted)	Specifies the number of packets discarded, errors encountered, packets overrun, carriers used, and collisions encountered.

What This Report Tells You

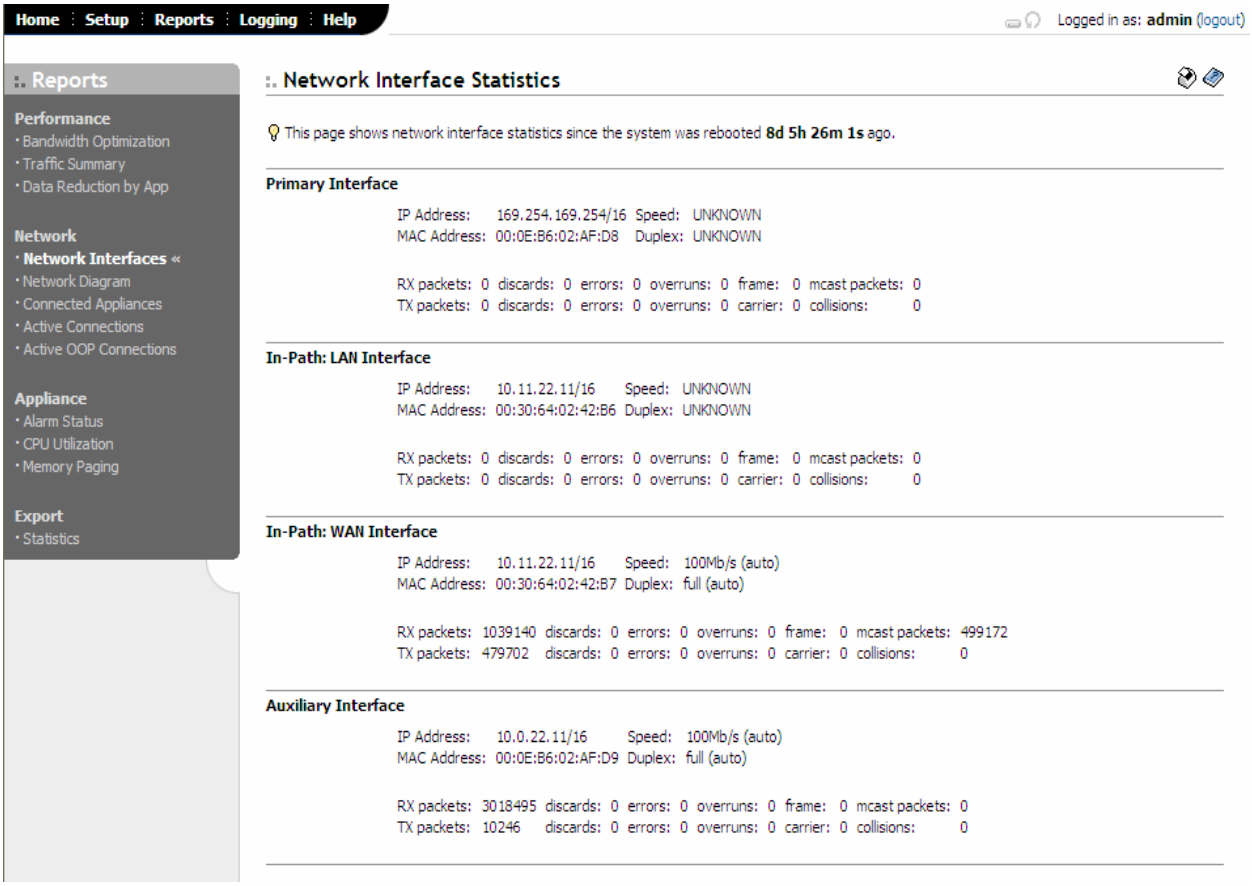
The Network Interface Statistics report answers the following questions:

- How many packets am I transmitting?
- How many errors are there in each transmission?
- What is the current status of my interface?

To view network interface statistics

1. Click the Reports tab to display the Reports: Performance Summary page.
2. Click in the Network Interfaces left menu to display the Reports: Network Interface Statistics page.

Figure 2-47. Reports: Network Interface Statistics Page



Viewing the Network Diagram

The Reports: Network Diagram report allows you to view a local network diagram of the interfaces and subnets in your HP system. The network diagram displays the following elements:

- In-path and out-of-path network configurations
- Primary and in-path subnets with network numbers
- Primary and in-path interface IP addresses
- WAN gateway IP address
- Single or multiple subnets
- Local HP EFS WAN Accelerator

The network diagram can be used as a troubleshooting tool for identifying:

- the interfaces that are not configured.
- whether the WAN gateway has been identified.

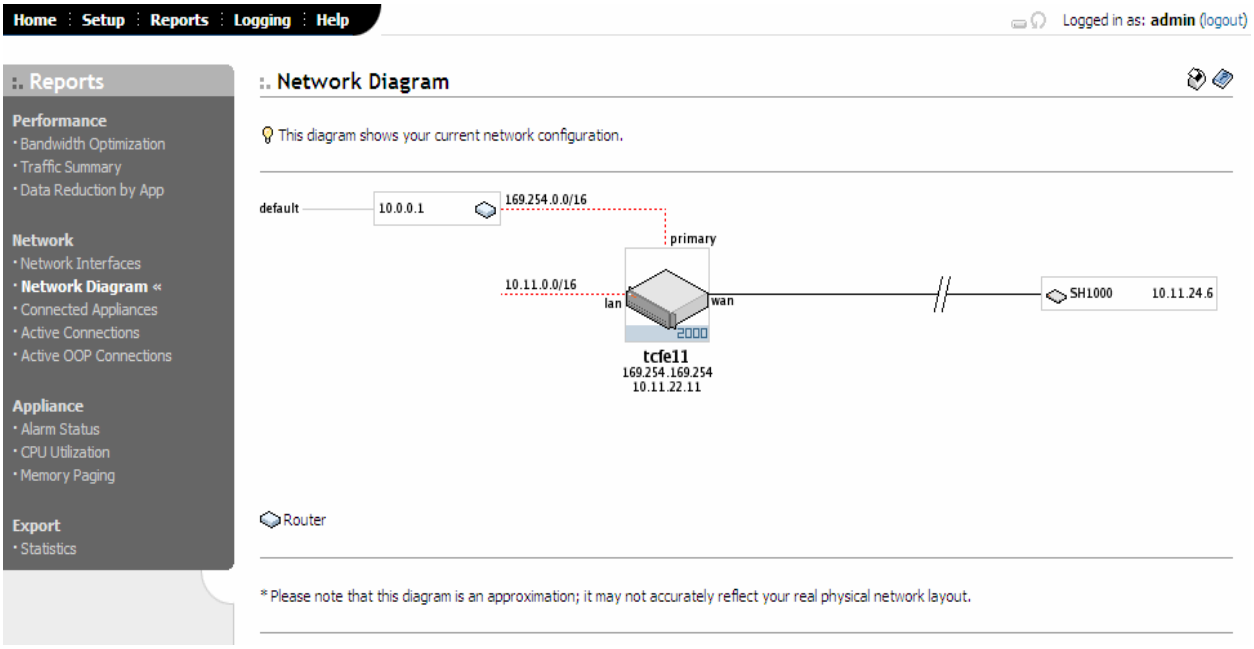
- whether links are down (for example, primary interface, WAN, and LAN).

The Reports: Network Diagram page also displays the connected HP EFS WAN Accelerators with their remote IP addresses and model type.

To view the current HP EFS WAN Accelerator network configuration

1. Click the Reports tab to display the Reports: Performance Summary page.
2. Click Network Diagram in the left menu to display the Reports: Network Diagram page.

Figure 2-48. Reports: Network Diagram Page



TIP: To print your report, click the **Printer** icon in the upper right corner of the page.

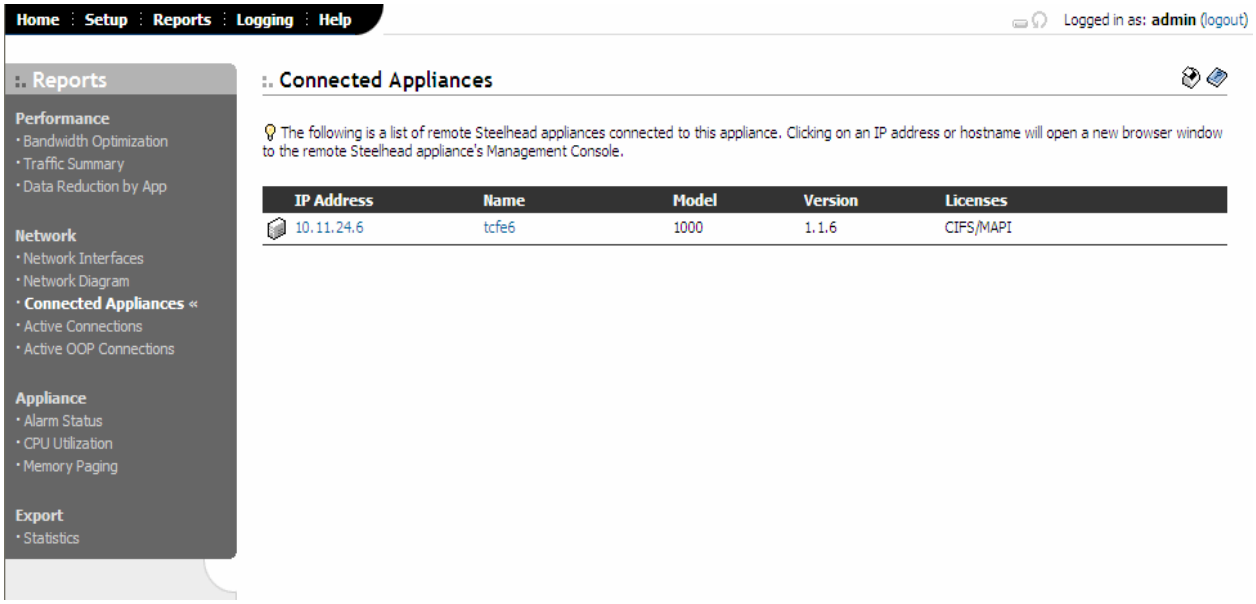
Viewing Connected HP EFS WAN Accelerators

You can view details about connected HP EFS WAN Accelerators in the Appliances: Connected Appliances page.

To view connected HP EFS WAN Accelerators

1. Click the Reports tab to display the Reports: Performance Summary page.
2. Click Connected Appliances in the left menu to display the Reports: Connected Appliances page.

Figure 2-49. Reports: Connected Appliances Page



TIP: To print your report, click the **Printer** icon in the upper right corner of the page.

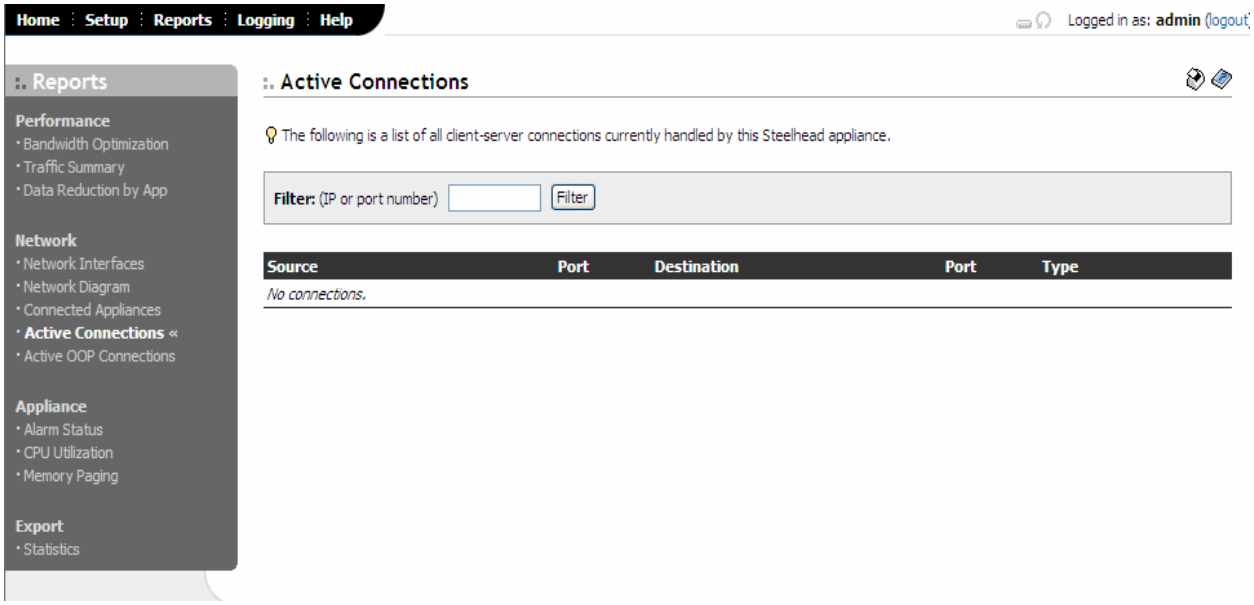
Viewing Active Connections

The Reports: Active Connections report displays the connections that are intercepted through the HP EFS WAN Accelerator, including the connections that are passed through unoptimized.

To view active connections

1. Click the Reports tab to display the Reports: Performance Summary page.
2. Click Active Connections in the left menu to display the Reports: Active Connections page.

Figure 2-50. Reports: Active Connections Page



TIP: Type an IP address or port number in the **Filter** text box to filter the report.

TIP: To print your report, click the **Printer** icon in the upper right corner of the page.

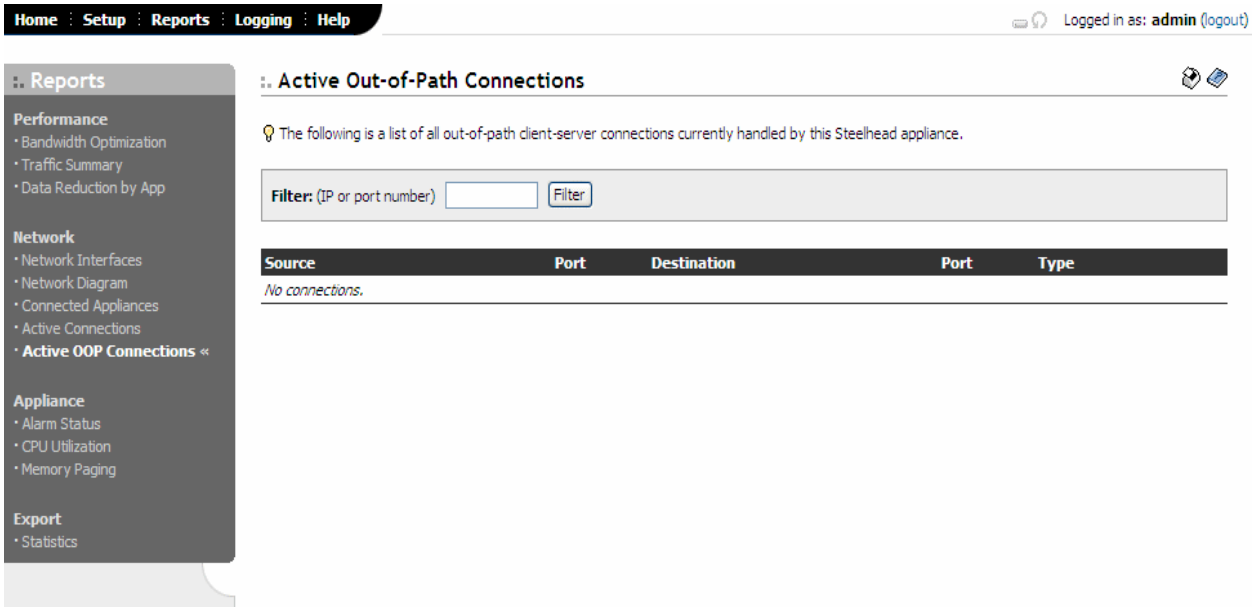
Viewing Active Out-of-Path Connections

The Reports: Active Out-of-Path Connections report displays the connections that are intercepted through the out-of-path HP EFS WAN Accelerator, including the connections that are passed through unoptimized.

To view active out-of-path connections

1. Click the Reports tab to display the Reports: Performance Summary page.
2. Click Active OOP Connections in the left menu to display the Reports: Active Out-of-Path Connections page.

Figure 2-51. Reports: Active Out-of-Path Connections Page



TIP: Type an IP address or port number in the **Filter** text box to filter the report.

TIP: To print your report, click the **Printer** icon in the upper right corner of the page.

Viewing Alarm Status Reports

The Reports: Alarm Status report summarizes the status of the following HP EFS WAN Accelerator alarms.

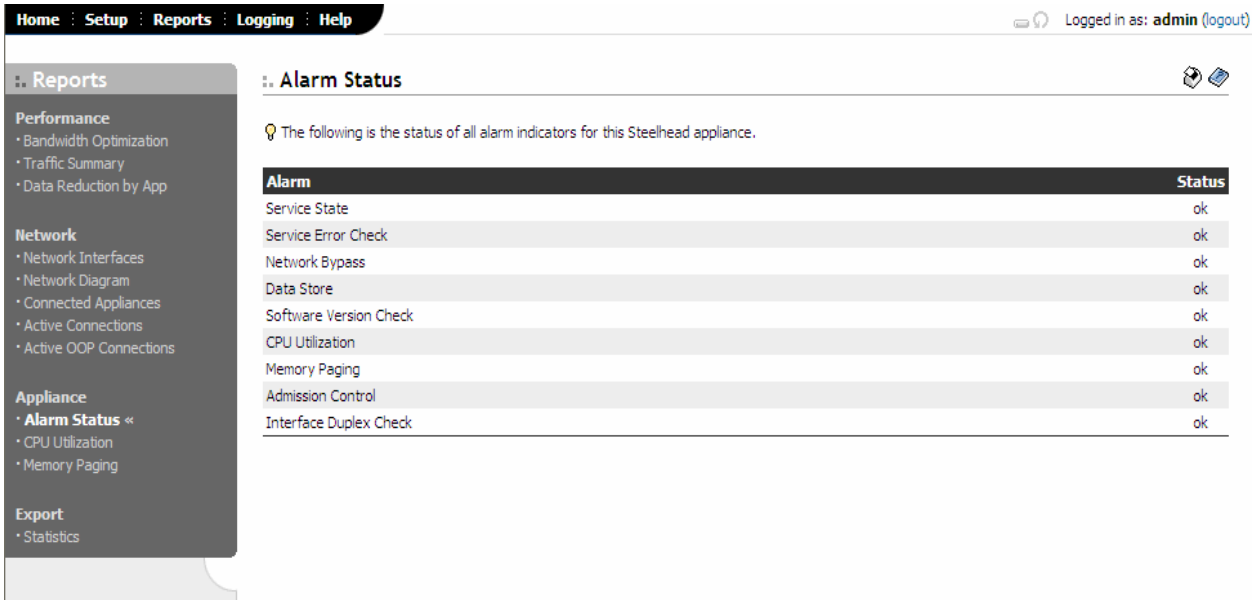
Alarm	Description
Service State	The current status of the HP EFS WAN Accelerator service. If the HP EFS WAN Accelerator is not running, restart the service. To restart the HP EFS WAN Accelerator service, at the bottom of the report, click **Click here**.
Service Error Check	The HP EFS WAN Accelerator has detected a software error in the HP EFS WAN Accelerator service. The HP EFS WAN Accelerator service continues to function, but an error message appears in the logs that you should investigate. To restart the HP EFS WAN Accelerator service, at the bottom of the report, click **Click here**.
Network Bypass	Whether the HP EFS WAN Accelerator is in bypass mode. If the HP EFS WAN Accelerator is in bypass mode, restart the HP EFS WAN Accelerator service. To restart the HP EFS WAN Accelerator service, at the bottom of the report, click **Click here**. If restarting the service does not resolve the problem, reboot the HP EFS WAN Accelerator. For detailed information, see "Rebooting the HP EFS WAN Accelerator" on page 95. If rebooting does not resolve the problem, shutdown and restart the HP EFS WAN Accelerator. For detailed information, see "Shutting Down the HP EFS WAN Accelerator" on page 96.
Data Store	Whether the data store is corrupt. To clear the data store of data, restart the HP EFS WAN Accelerator Service and click **Clear Data Store on Next Restart**. For detailed information, see "Starting, Stopping, and Restarting the HP EFS WAN Accelerator Service" on page 94.
Software Version Check	Whether there is a mismatch between software versions in the HP system. If a software mismatch is detected, resolve the mismatch by upgrading or reverting to a previous version of the software. For detailed information, see "Upgrading Your Software" on page 89.
Central Processing Unit (CPU) Utilization	Whether the system has reached the CPU threshold that you set. If the system has reached the CPU threshold, check your settings. For detailed information, see "Setting Alarm Thresholds" on page 63. If your alarm thresholds are correct, reboot the HP EFS WAN Accelerator. For detailed information, see "Rebooting the HP EFS WAN Accelerator" on page 95.
Memory Paging	Whether the system has reached the memory paging threshold that you set. If the system has reached the memory paging threshold, check your settings. For detailed information, see "Setting Alarm Thresholds" on page 63. If your memory thresholds are correct, reboot the HP EFS WAN Accelerator. For detailed information, see "Rebooting the HP EFS WAN Accelerator" on page 95.

Alarm	Description
Admission Control	Whether the system has been overloaded with connection requests and stops intercepting new connections to allow them to pass through. The alarm clears when the HP EFS WAN Accelerator moves out of that condition.
Interface Duplex Check	Whether the system has encountered a large number of packet errors in your network. Check the speed and duplex settings on the HP EFS WAN Accelerators on each side of your network. Make sure the speed and duplex settings on your HP EFS WAN Accelerators match the settings on your switch and router.
Redundant Array of Independent Disks (RAID)	Whether the system has encountered raid errors (for example, missing drives, pulled drives, drive failures, and drive rebuilds). For drive rebuilds, if a drive is removed and then reinserted, the alarm continues to be triggered until the rebuild is complete. **IMPORTANT**: Rebuilding a disk drive can take 4-6 hours. **NOTE**: RAID status applies only to the HP EFS WAN Accelerator, Models 3000 and 5000.

To view alarm status

1. Click the Reports tab to display the Reports: Performance Summary page.
2. Click Alarm Status in the left menu to display the Reports: Alarm Status page.

Figure 2-52. Reports: Alarm Status Page



TIP: If you have a service error check alarm, under Additional Information, click the **Click here** link to reset the alarm.

TIP: To print your report, click the **Printer** icon in the upper right corner of the page.

Creating CPU Utilization Reports

The Reports: System, CPU Utilization report summarizes the percentage of the CPU utilized in the time period specified.

The CPU Utilization report includes the following table of statistics that describe CPU activity for the time period you specify.

Field	Description
Average Utilization for CPU 1	Specifies the average CPU utilization.
Peak Utilization for CPU 1	Specifies the peak CPU utilization.

What this Report Tells You

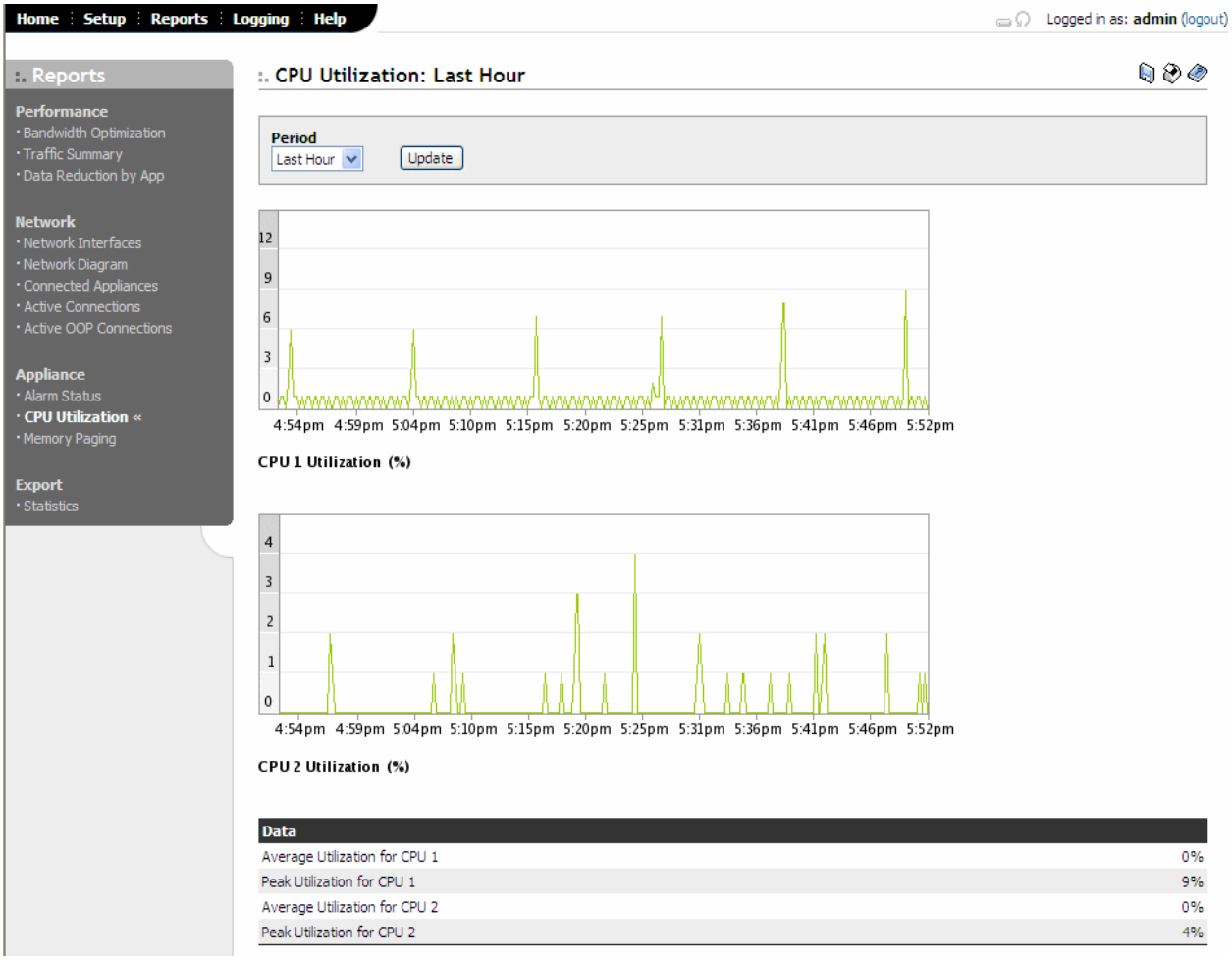
The CPU Utilization report answers the following questions:

- How much CPU am I using?
- What is the average and peak percentage of CPU that I am using?

To create the CPU Utilization report

1. Click the Reports tab to display the Reports: Performance Summary page.
2. Click CPU Utilization in the left menu to display the Reports: CPU Utilization page.

Figure 2-53. Reports: System, CPU Utilization Report



3. Select **Last Hour** or **Last Day** from the **Period** drop-down list.
4. Click **Update** to update your report.

TIP: To print your report, click the **Printer** icon in the upper right corner of the page.

TIP: Click the **Disk** icon in the upper right corner of the page to download your report statistics to your local disk in comma separated value (CSV) format. For detailed information about exporting statistics, see "Exporting Performance Statistics" on page 113.

Creating Memory Paging Reports

The Reports: Memory Paging report provides the total number of memory pages per second utilized in the time period specified.

The Memory Paging report includes the following table of statistics that describe memory paging activity for the time period you specify.

Field	Description
Average Pages Swapped Out	Specifies the average number of pages swapped. If 100 pages are swapped every couple of hours the HP EFS WAN Accelerator is functioning properly. If thousands of pages are swapped every few minutes, then you should contact technical support.
Peak Pages Swapped Out	Specifies the peak number of pages swapped.

What this Report Tells You

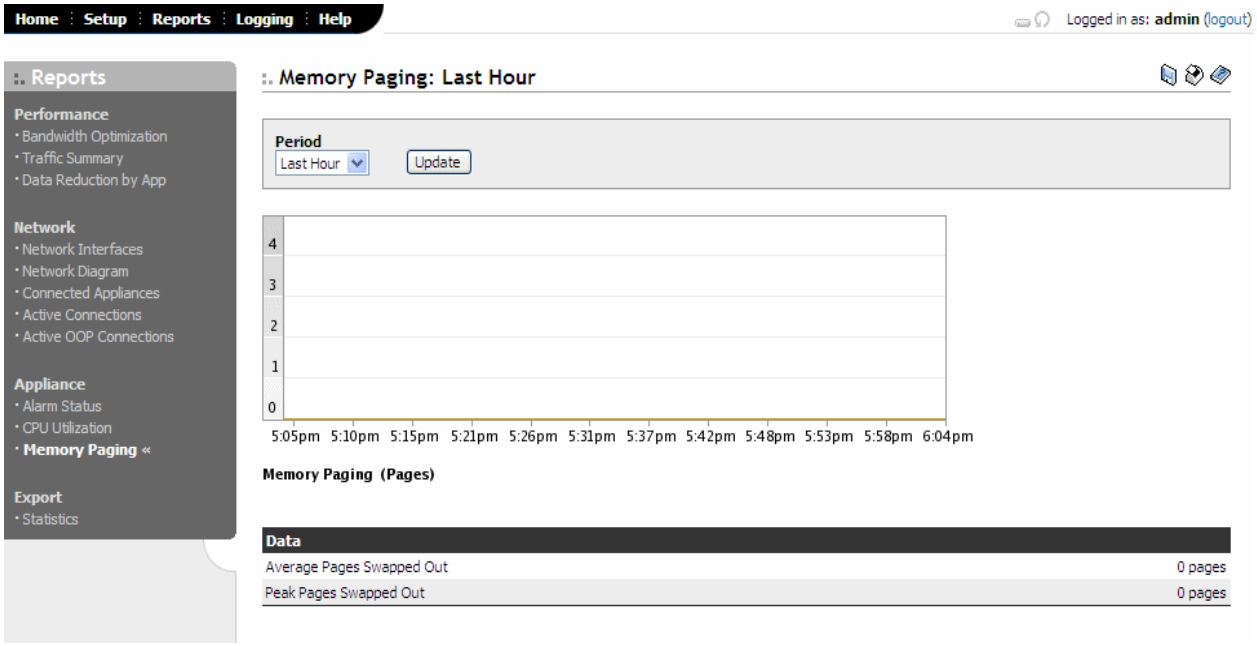
The Memory Paging report answers the following questions:

- How much memory am I using?
- What is the average and peak amount of memory pages swapped?

To create Memory Paging report

1. Click the Reports tab to display the Reports: Performance Summary page.
2. Click Memory Paging in the left menu to display the Reports: Memory Paging page.

Figure 2-54. Reports: Memory Paging Report



3. Select **Last Hour** or **Last Day** from the **Period** drop-down list.
4. Click **Update** to update your report.

TIP: To print your report, click the **Printer** icon in the upper right corner of the page.

TIP: Click the **Disk** icon in the upper right corner of the page to download your report statistics to your local disk in comma separated value (CSV) format. For detailed information about exporting statistics, see "Exporting Performance Statistics" on page 113.

Exporting Performance Statistics

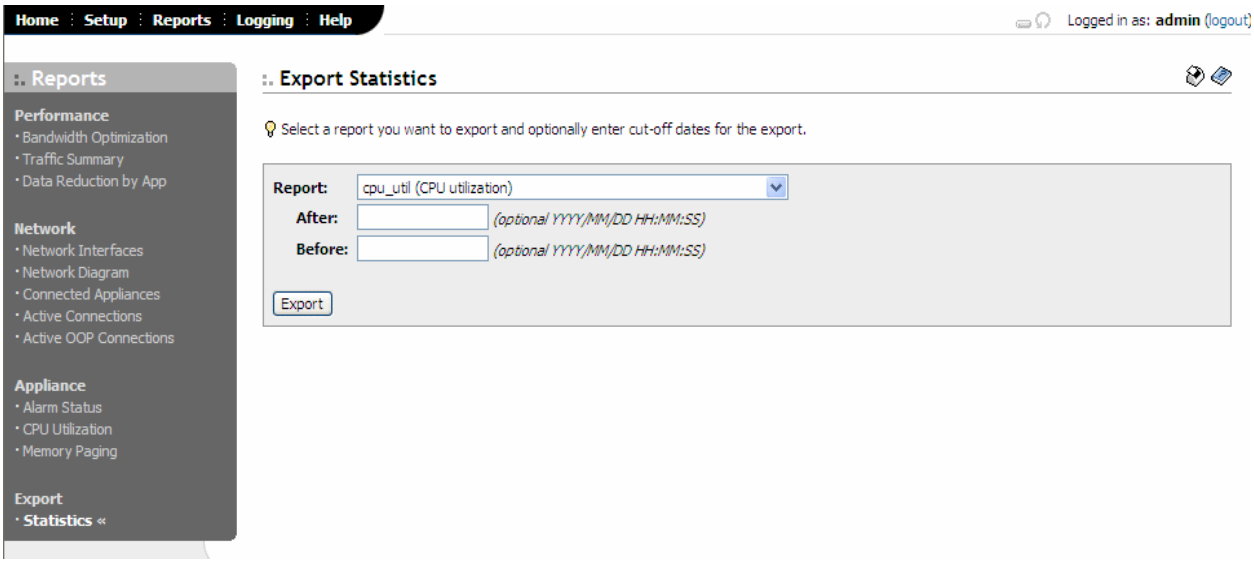
You can export performance statistics in comma separated value (CSV) format in the Reports: Export page. The CSV format allows you to easily import the statistics into spreadsheets and databases. You can open the CSV file in any text editor.

The CSV file contains commented lines (comments beginning with the # character) at the top of the file. These comments report what host generated the file, the report that was generated, time boundaries, the time the export occurred, and the version of the HP EFS WAN Accelerator the file was exported from. The statistical values are provided in columns: the first column is the date and time of the statistic sample, the columns that follow contain the data.

To export statistics

1. Click the Reports tab to display the Reports: Performance Summary page.
2. Click Statistics in the left menu to display the Reports: Export Statistics page.

Figure 2-55. Reports: Export Statistics Page



3. Select the report you want to export from the **Report** drop-down list.

4. Optionally, type a date and time from which the statistics should begin in the **After** text box. Use the following format: YYYY/MM/DD HH:MM:SS.

5. Optionally, type a date and time from which the statistics should end in the **Before** text box. Use the following format: YYYY/MM/DD HH:MM:SS.

TIP: To print your report, click the **Printer** icon in the upper right corner of the page.

Viewing HP EFS WAN Accelerator Logs

The following section describes how to view HP EFS WAN Accelerator logs.

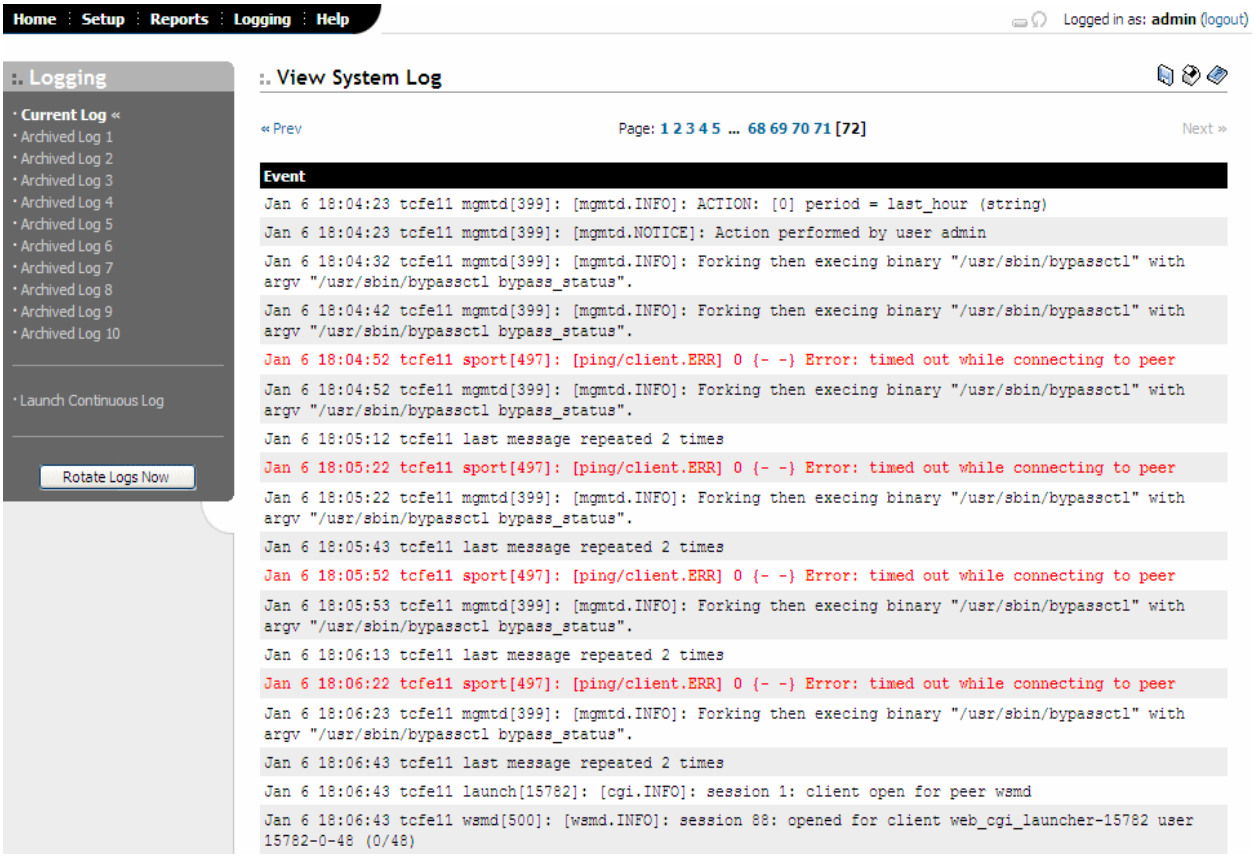
Viewing HP EFS WAN Accelerator Logs

You can view HP EFS WAN Accelerator logs in the Logging: View System Log page. Use system logs to monitor HP EFS WAN Accelerator activity and to troubleshoot problems with the appliance. The most recent log events are listed first.

To view HP EFS WAN Accelerator logs

1. Click the Logging tab to display the Logging: View System Log page.

Figure 2-56. Logging: View System Log Page



2. Below the Event list, click the page number to view additional pages for the log. To view previous pages, click **Prev**.

TIP: Click the **Disk** icon in the upper right corner to download the log file to your local machine.

TIP: In the left menu, click **Launch Continuous Log**, to display continuous log messages in your Web browser. This feature might not be supported in all Web browsers.

TIP: In the left menu, click **Rotate Logs Now** to archive the current log.

Getting Help

The Help tab provides you with the following links to help you administer and manage the HP EFS WAN Accelerator:

- **Technical Support**. HP technical support.
- **CLI Commands**. The HP EFS WAN Accelerator Command Line Interface.
- **Online Help.** A table of contents of the help topics in the Management Console.

Contacting Technical Support

You can obtain the technical support phone number and email address from the Help: Technical Support page.

To email technical support

1. Click the Help tab to display the Help: Technical Support page.
2. Click the email link to display a blank email message in a new window.

TIP: Under Email, click the email link to email a message to HP Technical Support.

TIP: Under Website, click the Web site link to go to the HP Technical Support Web site.

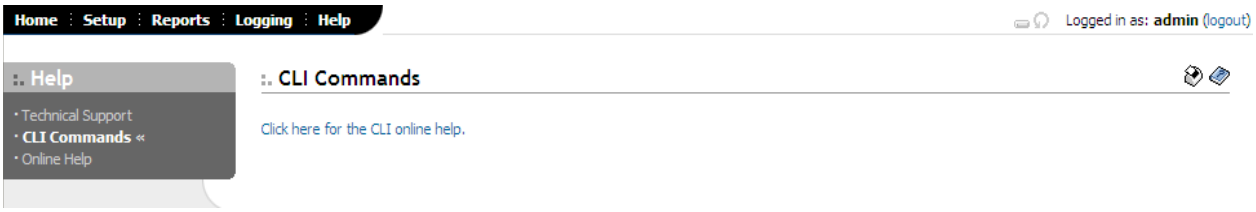
Viewing CLI Commands

You can view a reference manual for the HP EFS WAN Accelerator CLI commands in the Help: CLI Commands page.

To view CLI commands

1. Click the Help tab to display the Help: Technical Support page.
2. Click CLI Commands in the left menu to display the Help: CLI Commands page.

Figure 2-57. Help: CLI Commands Page



3. Click the **Click here for the CLI online help** link to go to the HP EFS WAN Accelerator Command Line Interface. The manual appears in a new window.

TIP: To print the guide, click **PDF** in the upper right corner.

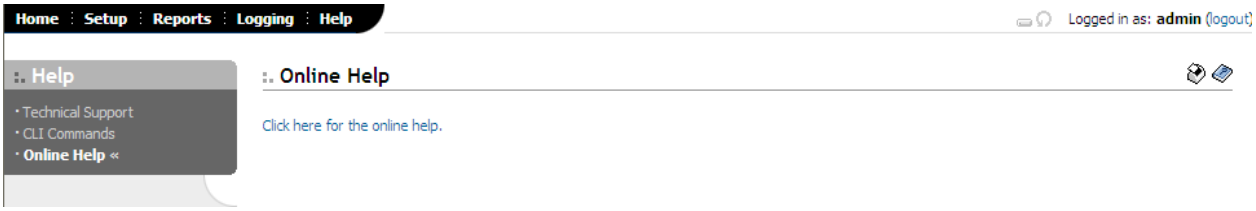
Viewing Online Help Contents

You can view the table of contents for online help in the Help: Online Help page. The online help contains page-level help for each page in the Management Console.

To view online help contents

1. Click the Help tab to display the Help: Technical Support page.
2. Click Online Help in the left menu to display the Help: Online Help page.

Figure 2-58. Help: Online Help Page



3. Click the **Click here for online help** link to display the online help table of contents.

APPENDIX A

HP EFS WAN Accelerator Ports

In This Appendix

This appendix describes the HP EFS WAN Accelerator default, secure, and interactive ports. It contains the following sections:

Default Ports

The HP EFS WAN Accelerator uses the following default ports.

- In-Path Listening Port: 7800
- Out-of-Path Server Port: 7810
- Failover Port: 7820
- Exchange Port: 7830

Commonly Optimized Ports

The HP EFS WAN Accelerator by default optimizes all ports. If you do not want the HP EFS WAN Accelerator to optimize all ports for an in-path or out-of path configuration, you can specify specific ports for optimization.

Although these ports can vary according to your requirements, the following ports are commonly specified for in-path and out-of-path configurations:

- 80
- 135
- 139
- 445
- 7830

Interactive Ports Automatically Forwarded by the HP EFS WAN Accelerator

The following interactive ports are automatically forwarded by the HP EFS WAN Accelerator by the HP EFS WAN Accelerator when you enable forwarding of interactive ports in the Management Console.

Port	Description
7	TCP ECHO
23	Telnet
37	UDP/Time
107	Remote Telnet Service
513	Remote Login
514	Shell
3389	MS WBT Server, TS/Remote Desktop
5631	PC Anywhere
5900-5903	VNC
6000	X11

For detailed information about how to set interactive port forwarding, see the "Passing-Through Traffic on Secure and Interactive Ports" on page 47.

Secure Ports Automatically Forwarded by the HP EFS WAN Accelerator

The following tables contain the secure ports that are automatically forwarded by the HP EFS WAN Accelerator when you enable forwarding of secure ports in the Management Console.

For detailed information about how to enable forwarding of secure ports, see the "Passing-Through Traffic on Secure and Interactive Ports" on page 47.

Type	Port	Description
ssh	22/tcp	SSH Remote Login Protocol
https	443/tcp	http protocol over TLS/SSL
smtps	465/tcp	SMTP over SSL (TLS)
nntps	563/tcp	nntp protocol over TLS/SSL (was snntp)
imap4-ssl	585/tcp	IMAP4+SSL (use 993 instead)
sshell	614/tcp	SSLshell
ldaps	636/tcp	ldap protocol over TLS/SSL (was sldap)
ftps-data	989/tcp	ftp protocol, data, over TLS/SSL
ftps	990/tcp	ftp protocol, control, over TLS/SSL
telnets	992/tcp	telnet protocol over TLS/SSL
imaps	993/tcp	imap4 protocol over TLS/SSL
pop3s	995/tcp	pop3 protocol over TLS/SSL (was spop3)
l2tp	1701/tcp	l2tp
pptp	1723/tcp	pptp
tftps	3713/tcp	TFTP over TLS

The following table contains the uncommon ports automatically forwarded by the HP EFS WAN Accelerator.

Type	Port	Description
nsiiops	261/tcp	IIOP Name Service over TLS/SSL
ddm-ssl	448/tcp	DDM-Remote DB Access Using Secure Sockets
corba-iiop-ssl	684/tcp	CORBA IIOP SSL
ieee-mms-ssl	695/tcp	IEEE-MMS-SSL
ircs	994/tcp	irc protocol over TLS/SSL
njenet-ssl	2252/tcp	NJENET using SSL
ssm-cssps	2478/tcp	SecurSight Authentication Server (SSL)
ssm-els	2479/tcp	SecurSight Event Logging Server (SSL)
giop-ssl	2482/tcp	Oracle GIOP SSL
ttc-ssl	2484/tcp	Oracle TTC SSL
syncserverssl	2679/tcp	Sync Server SSL
dicom-tls	2762/tcp	DICOM TLS
realsecure	2998/tcp	Real Secure
orbix-loc-ssl	3077/tcp	Orbix 2000 Locator SSL

Type	Port	Description
orbix-cfg-ssl	3078/tcp	Orbix 2000 Locator SSL
cops-tls	3183/tcp	COPS/TLS
csvr-sslproxy	3191/tcp	ConServR SSL Proxy
xnm-ssl	3220/tcp	XML NM over SSL
msft-gc-ssl	3269/tcp	Microsoft Global Catalog with LDAP/SSL
networklenss	3410/tcp	NetworkLens SSL Event
xtrms	3424/tcp	xTrade over TLS/SSL
jt400-ssl	3471/tcp	jt400-ssl
seclayer-tls	3496/tcp	securitylayer over tls
vt-ssl	3509/tcp	Virtual Token SSL Port
jboss-iiop-ssl	3529/tcp	JBoss IIOP/SSL
ibm-diradm-ssl	3539/tcp	IBM Directory Server SSL
can-nds-ssl	3660/tcp	Candle Directory Services using SSL
can-ferret-ssl	3661/tcp	Candle Directory Services using SSL
linktest-s	3747/tcp	LXPRO.COM LinkTest SSL
asap-tcp-tls	3864/tcp	asap/tls tcp port
topflow-ssl	3885/tcp	TopFlow SSL
sdo-tls	3896/tcp	Simple Distributed Objects over TLS
sdo-ssh	3897/tcp	Simple Distributed Objects over SSH
iss-mgmt-ssl	3995/tcp	ISS Management Svcs SSL
suucp	4031/tcp	UUCP over SSL
wsm-server-ssl	5007/tcp	wsm server ssl
sip-tls	5061/tcp	SIP-TLS
imqtunnels	7674/tcp	iMQ SSL tunnel
davsrcs	9802/tcp	WebDAV Source TLS/SSL
intrepid-ssl	11751/tcp	Intrepid SSL
rets-ssl	12109/tcp	RETS over SSL

Glossary

ARP. Address Resolution Protocol. An IP protocol used to obtain a node's physical address.

Bandwidth. The upper limit on the amount of data, typically in kilobits per second (kbps), that can pass through a network connection. Greater bandwidth indicates faster data transfer capability.

Bit. A Binary digit. The smallest unit of information handled by a computer; either 1 or 0 in the binary number system.

Blade. One component in a system that is designed to accept some number of components (blades).

CIFS. Common Internet File System. CIFS is the remote file system access protocol used by Windows servers and clients to share files across the network.

Default gateway. The default address of a network or web site. It provides a single domain name and point of entry to the network or site.

DHCP. Dynamic Host Configuration Protocol. Software that automatically assigns IP addresses to client stations logging onto a TCP/IP network.

Domain. In the Internet, a portion of the Domain Name Service (DNS) that refers to groupings of networks based on the type of organization or geography.

DNS. Domain Name Service. System used in the Internet for translating names of network nodes into IP addresses. A Domain Name Server notifies hosts of other host IP addresses, associating host names with IP addresses.

Ethernet. The most widely used Local Area Network (LAN) access method.

Gateway. A computer that acts as an intermediate device with two or more networks that use the same protocols. The gateway functions as an entry and exit point to the network. Transport protocol conversion might not be required, but some form of processing is typically performed.

Gigabit Ethernet. An Ethernet technology that raises transmission speed to 1 Gbps (1000 Mbps).

Host. A computer or other computing device that resides on a network.

Host address. The IP address assigned to each computer attached to the network.

Host name. Name given to a computer, usually by DNS.

HTTP. HyperText Transport Protocol. The protocol used by Web browsers to communicate with Web servers.

HTTPS. HyperText Transport Protocol Secure.The protocol for accessing a secure Web server. Using HTTPS directs the message to a secure port number to be managed by a security protocol

Interface. The point at which a connection is made between two elements, systems, or devices so that they can communicate with one another.

Internet. The collection of networks tied together to provide a global network that use the TCP/IP suite of protocols.

IP. Internet protocol. Network layer protocol in the TCP/IP stack that enables a connectionless internetwork service.

IP address. In IP version 4 (IPv4), a 32-bit address assigned to hosts using the IP protocol. Also called an Internet address.

Latency. Delay between a request being issued and its response being received.

Layer 4. A communications protocol (called the transport layer) responsible for establishing a connection and ensuring that all data has arrived safely. The application delivers its data to the communications system by passing a stream of data bytes to the transport layer along with the socket (the IP address of the station and a port number) of the destination machine.

MAPI. Messaging API. A programming interface from Microsoft that enables a client application to send and receive mail from Exchange Server or a Microsoft Mail (MS Mail) messaging system. Microsoft applications such as Outlook, the Exchange client, and Microsoft Schedule use MAPI.

Microsoft Exchange. Messaging and groupware software for Windows from Microsoft. The Exchange server is an Internet-compliant messaging system that runs under Windows systems and can be accessed by Web browsers, the Windows Inbox, Exchange client or Outlook. The Exchange server is also a storage system that can hold anything that needs to be shared.

Netmask. A 32-bit mask which shows how an Internet address is divided into network, subnet, and host parts. The netmask has ones in the bit positions in the 32-bit address which are used for the network and subnet parts, and zeros for the host part. The mask must contain at least the standard network portion

(as determined by the class of the address), and the subnet field should be contiguous with the network portion.

NFS. Network File System. The file sharing protocol in a UNIX network.

NIS. Network Information Services. A naming service from that allows resources to be easily added, deleted or relocated.

Packet. A unit of information transmitted, as a whole, from one device to another on a network.

Probe. A small utility program that is used to investigate, or test, the status of a system, network or Web site.

Policy. Routing and Quality of Service (QoS) scheme that forwards data packets to network interfaces based on user-configured parameters.

Port. A pathway into and out of the computer or a network device such as a hub, switch, or router. On network devices, the ports are for communications, typically connecting Ethernet cables or other network devices.

Router. A device that forwards data packets from one LAN or WAN to another. Based on routing tables and routing protocols, routers read the network address in each transmitted frame and make a decision on how to send it based on the most expedient route (traffic load, line costs, speed, bad lines, etc.). Routers work at Layer 3 in the protocol stack, whereas bridges and switches work at the Layer 2.

SNMP. Simple Network Management Protocol. A network protocol that provides a way to monitor network devices, performance, and security and to manage configurations and collect statistics.

Switch. A network device that filters and forwards frames based on the destination address of each frame. The switch operates at Layer 2 (data link layer) of the Open System Interconnection (OSI) model.

TCP. Transmission Control Protocol. The error correcting Transport layer (Layer 4) in the TCP/IP protocol suite.

TCP/IP. Transmission Control Protocol/Internet Protocol. The protocol suite used in the Internet, intranets, and extranets. TCP provides transport functions, which ensures that the total amount of bytes sent is received correctly at the other end. TCP/IP is a routable protocol, and the IP part of TCP/IP provides this capability.

Index